RĂZBOIUL TĂCUT

Privire asupra lumii informațiilor

ABRAM N. SHULSKY şi GARY J. SCHMITT

Ediția a 3-a

POTOMAC BOOKS
Washington D.C.

CUPRINS

Prefață / 5

Către cititor / 7

Introducere: Scriind despre secrete / 9

1. **Ce este activitatea de informații? / 12**

   Delimitarea domeniului / 14
   Serviciile secrete în era informațiilor / 18
   Elementele culegerii de informații / 19

2. **Spioni, maşini şi biblioteci: culegerea de informații / 22**

   Culegerea de informații din surse umane / 22
   Culegerea de informații din surse tehnice / 34
   Comparații între Humint şi Techint / 47
   Culegerea de informații din surse deschise / 52

3. **Care este semnificația informațiilor? Analiza şi prelucrarea / 55**

   Ce este analiza? / 55
   Produsul activității de informații / 71
   Eşecurile serviciilor de informații şi evenimentele neprevăzute / 77

4. **În culise: Operațiunile secrete / 90**

   Ce este o operațiune secretă? / 90
   Tipuri şi exemple de operațiuni secrete / 92
   Acțiunile secrete şi păstrarea confidențialității / 108
   Acțiunile secrete şi culegerea de informații / 112

5. **Spion contra spion: Contra-informațiile / 116**

   Clasificarea informațiilor / 116
   Contraspionajul / 126
   Activități contrainformative multidisciplinare (MDCI) / 132
   Dezinformare şi contra-dezinformare / 135
   Analiza contrainformativă / 145

6. **Controlul paznicilor: Managementul culegerii de informații / 147**

Caracterul secret şi controlul / 147
Expertiză şi strategie / 151
Serviciile de informații în "era informațiilă" / 160
Activitatea de informații şi democrația / 163

7. **Două perspective asupra lumii informațiilor / 180**

Istoricul viziunii americane / 182
Activitatea de informații şi problemele etice / 189

8. **Elemente pentru o teorie a culegerii informațiilor / 191**

Note / 199

Despre autori / 267

PREFAȚĂ

Războiul tăcut își are originea într-un curs de culegere de informații, pe care l-am predat în 1985, când eram profesor asociat la Centrul John M. Olin de Studiu al Teoriei și Practicilor Democratice, Universitatea Chicago. Întoarcerea la lumea academică mi-a impus o organizare mai clară a ideilor mele privind lumea informațiilor, subiect pe care-l cunoșteam în virtutea carierei mele de la Washington. Cartea a fost publicată pentru prima dată în 1991. La scurt timp, promovarea unor noi legi privind activitatea de informații, atât în SUA cât și în alte țări, publicarea mai multor lucrări pe aceeași temă și destrămarea URSS au determinat publicarea unei ediții revizuite a *Războiului tăcut.* Dar la momentul respectiv mă întorsesem deja la postul meu de oficial guvernamental la Ministerul Apărării și nu aveam suficient timp pentru a face adăugirile necesare. De aceea, l-am rugat pe Gary Schmitt, cel care m-a înlocuit în postul de director de personal la Comisia Parlamentară de Control a Serviciilor de Informații și fost director executiv al Comitetului de Consultanță a Președintelui privind Informațiile Externe, să se ocupe de revizuirea cărții. A doua ediție a apărut în 1993.

În această perioadă, bibliografia și resursele dedicate subiectului s-au diversificat. În plus, a existat o efervescență în domeniul legislativ care a dus la promovarea unor legi speciale pentru domeniul informațiilor în vederea armonizării reglementărilor deja existente cu cerințele guvernării democratice. Cum va fi influențată culegerea de informații – o activitate guvernamentală care are ca rol principal culegerea, protejarea și transmiterea informațiilor – de aceste aspecte privind disponibilitatea și transmiterea informațiilor, acesta este ceea ce încercăm să urmărim în a 3-a ediție a lucrării de față.

Deși *Războiul tăcut* a fost revizuită și completată de două ori până acum, subiectul, structura și conținutul de bază al cărții au rămas neschimbate. *Războiul tăcut* nu este o prezentare istorică a activității de informații desfășurate de un anumit guvern. Cu toate că cele mai multe dintre exemplele folosite în carte sunt extrase din experiența serviciilor britanice și americane, rolul lor este de a prezenta concepte generale și chestiuni ce definesc activitatea de informații. Sfârșitul Războiului Rece, debutul unei noi ere strategice și riscurile aduse de "era informațională" vor determina, evident, schimbări la nivelul practicilor și solicitărilor ce țin de serviciile de informații. Însă ceea ce-și propune să demonstreze lucrarea de față este faptul că lumea informațiilor este strâns legată de concurența dintre state și că, în lipsa acelei stări de "pace perpetuă" atât de dragă lui Kant,

informațiile rămân, alături de diplomație şi forțele militare, instrumente de guvernare. În acest sens, atât cetățeanul cât şi studentul, trebuie să înțeleagă că elementele de bază ale activității de informații, interacțiunile, tensiunile şi relația uneori dificilă dintre servicii şi guvernul democratic, precum şi între servicii şi societate au ca scop final îmbunătățirea securității.

La ediția aceasta, ca şi la cele anterioare, au contribuit şi au adus completări, precizări, comentarii numeroşi studenți, prieteni şi colegi. Mulțumiri lui Eliot A. Cohen, Kenneth E. de Graffenreid, Hillel G. Fradkin, Sam Halperin, Sheila Kerr, Carnes R. Lord, Kenneth Robertson şi Diane S. Roark. Prima ediție a cărții a fost scrisă în perioada în care lucram la Biroul pentru Strategii Naționale de Informații, perioadă în care am beneficiat de grant-urile Fundației John M. Olin şi Fundația Lynde şi Harry Bradley. Cea ce a doua ediție a fost revizuită de Gary care este angajat al NSIC. Mulțumiri speciale lui Roy Godson, preşedintele NSIC, şi Jeffrey Berman, director al NSIC.

Abram N. Shulsky
Washington, DC

CĂTRE CITITOR

Nu s-a făcut nici o revizuire a textului în urma atacurilor teroriste din 11 Septembrie 2001, moment în care lucrarea noastră era deja pregătită pentru tipar. Sigur, va dura un timp până când se vor vedea implicaţiile acestor evenimente. Totuşi este evident că se va acorda mai multă atenţie culegerii de informaţii din surse umane în vederea contracarării unor potenţiale atacuri teroriste; în plus se vor accepta din ce în ce mai mult acoperiri "neoficiale" pentru ofiţerii de informaţii. Legile privind securitatea internă se vor diversifica, iar chestiunile privind interceptările şi supravegherea operativă vor deveni subiecte de interes din perspectiva întrebării dacă individul sau grupul pot fi supuşi monitorizării în baza unei decizii politice, chiar dacă nu există nici o dovadă a comiterii unei infracţiuni.

INTRODUCERE:

Scriind despre secrete

În cursul ultimului sfert de secol, serviciile de informaţii – în ciuda faptului că una dintre caracteristicile lor esenţiale rămâne conspirativitatea – au început să apară tot mai des în presă şi să facă obiectul a numeroase studii şi cercetări ştiinţifice. Dezbaterile şi întrebările despre servicii nu mai constituie motiv doar de scandal şi discuţii în contradictoriu. Acestea au fost acceptate ca un aspect normal al dezbaterilor publice privind activităţile guvernamentale în genere.

Deşi dezbaterile publice despre evenimentele obişnuite din domeniul culegerii de informaţii depind în continuare, în mare măsură, de materialul brut privind "scurgerile" autorizate sau neautorizate de informaţii clasificate, literatura de specialitate a luat amploare. Simpla trecere a timpului, amplificată de o mai mare deschidere din partea multor guverne democratice, a dus la declasificarea unei mari părţi din materialele istorice legate de al doilea Război Mondial şi de Războiul Rece. În plus, căderea comunismului în fosta Uniune Sovietică şi în Europa de Est a făcut posibil accesul în vederea studierii unor arhive, în special în fosta RDG, şi, în mai mică măsură, în Rusia. Abordarea "dimensiunii" de intelligence devine o practică comună în ce priveşte, în special, istoria diplomatică şi militară.

Intensificarea dezbaterilor publice pe probleme privind culegerea de informaţii în general nu au condus, totuşi, la o mai bună înţelegere a acestui domeniu. Într-adevăr, dezbaterile publice recente privind culegerea de informaţii sunt caracterizate de o neglijare a întrebărilor fundamentale despre rolul pe care trebuie să îl aibă serviciile de informaţii şi conspirativitatea într-o democraţie. Într-un sens mai general, exceptând câteva lucrări de specialitate care au coincis cu ultima încercare majoră a Congresului american de a "reforma" serviciile de informaţii (la începutul anilor '90), abordarea publică a aspectelor legate de culegerea de informaţii, atunci când nu au avut nicio încărcătură istorică, a fost similară abordării specifice cazurilor de spionaj.

Aceasta contrastează cu valul timpuriu de literatură privind domeniul culegerii de informaţii din anii '70 şi începutul anilor '80. În acea perioadă, mare parte a dezbaterilor publice privind serviciile – mai ales în Statele Unite, dar cu ecouri şi în alte ţări democratice – putea fi catalogată ca aparţinând uneia dintre cele două tabere care se diferenţiau prin abordările lor faţă de ideea fundamentală privind rolul serviciilor de informaţii într-o societate democratică şi relaţia dintre conspirativitate şi normele guvernării democratice.

Potrivit uneia dintre tabere, serviciile de informaţii au devenit sau, cel puţin, ar fi trebuit să devină mai puţin nişte instituţii "de capă şi spadă" şi, mai curând, o sferă a ştiinţelor sociale care să caute să analizeze şi în final să anticipeze problemele de natură politică, economică, socială şi militară.

Prin urmare, nu era nevoie să desfăşoare o activitate prin definiţie secretă. Dacă pentru a proteja sursele unor informaţii importante este nevoie de conspirativitate, aspectele esenţiale privind mişcările politice, economice, sociale, tehnologice şi demografice care conturează direcţia în care se îndreaptă un stat pe termen lung nu ar trebui să constituie un mare secret![1] Astfel, nu numai că problemele privind domeniul informaţiilor ar putea fi dezbătut public fără dificultate, dar, prin demistificarea acestui domeniu şi încurajarea schimbului de idei între comunităţile de informaţii şi cele academice, dezbaterile publice ar putea ajuta serviciile de informaţii să-şi atingă şi chiar să-şi depăşească scopul de a deveni o ştiinţă socială (serviciile de informaţii devenind, mai curând, "grupuri consultative de experţi").[2]

Potrivit celeilalte tabere, articolele despre culegerea de informaţii au ca scop să dezvăluie eventuale ilegalităţi şi erori şi să contribuie la schimbarea în mai bine a modului în care agenţiile operează.[3] Din această perspectivă, conspirativitatea în care erau învăluite operaţiunile serviciilor secrete a fost, fie cauza unor ilegalităţi, fie o precondiţie necesară a acestora. Prin urmare, dezbaterile publice pe marginea problemelor privind culegerea de informaţii au constituit un remediu în sine. Indiferent ce prejudiciu ar fi adus dezvăluirea unor secrete legitime, acest lucru era considerat nesemnificativ comparativ cu prejudiciile pe care le-ar putea aduce chiar serviciile secrete, operând dincolo de ochiul critic al publicului. Aşadar, dezvăluirea de informaţii despre un serviciu secret "ne-reformat" nu constituia o problemă – deşi s-ar fi găsit voci care să afirme că, departe de ochii opiniei publice, orice astfel de organizaţie se poate abate de la scopurile ei iniţiale.

În ultima perioadă, majoritatea studiilor şi cercetărilor în domeniu s-au axat pe relatări istorice privind activităţile specifice de culegere a informaţiilor.[4] Dezbaterile pe marginea mai multor aspecte curente au fost dominate de relatarea unor cazuri de spionaj, accentul punându-se mai degrabă pe acuzaţiile de incompetenţă decât pe abuzurile de natură etică sau politică.[5] Aceste lucrări nu aveau tendinţa de a marca puncte politice sau ideologice (în afară de faptul evident, se pare, că este mai bine să avem un serviciu de informaţii competent decât unul incompetent).

Războiul tăcut îşi propune să dea răspunsul la o serie de întrebări. Încearcă să abordeze conceptele fundamentale în înţelegerea lumii culegerii de informaţii. Scopul este acela de a da cititorului posibilitatea să mediteze la aspectele generale ale politicii de culegere de informaţii astfel încât să înţeleagă complexitatea şi ambiguităţile inerente acestei sfere de activitate. De aceea, abordarea este una fundamental teoretică; pentru a ilustra aspectele generale sunt utilizate detalii cunoscute despre activitatea reală a serviciilor de informaţii[6]; nu se face nici o încercare de înţelegere a trecutului serviciilor sau a statutului actual al acestora.

Acesta este motivul pentru care această carte se poate baza pe informaţiile publice privind activităţile de culegere a informaţiilor.[7] Nu au existat nici un fel de încercări de furnizare de informaţii care să nu fie deja cunoscute publicului. Acest lucru se datorează, în parte, faptului că am

primit drept de acces la informații clasificate ce priveau diferite poziții din cadrul conducerii SUA (totuşi, nu şi din cadrul vreunui serviciu secret). Ca o pre-condiție a dreptului de acces, am promis să nu dezvăluim astfel de informații.[8]

Ce este şi mai important, considerăm confidențialitatea ca fiind esențială în operațiunile de intelligence şi, în orice caz, nu credem că simpla publicare a unor amănunte despre misiunile serviciilor secrete americane este de bun augur. Majoritatea acestor detalii nu par să ridice probleme de politică publică importante sau să fie necesare în înțelegerea conceptelor fundamentale de culegere a informațiilor pe care le avem în vedere în prezenta carte.

Deşi culegerea de informații devine un domeniu de studiu ştiințific recunoscut, mai ales în lumea occidentală, teoretizarea pe marginea acestuia rămâne într-un stadiu incipient. Prin această carte încercăm să reducem acest neajuns. În acelaşi timp, trebuie să admitem că, raportându-se în mare parte la experiența anglo-americană, această carte este departe de a oferi o "teorie a culegerii de informații" general valabilă. Această raportare se datorează în mare parte faptului că cele mai multe informații publice despre culegerea de informații se referă, deloc surprinzător, la serviciile secrete ale acelor țări care dispun de cele mai deschise sisteme politice. Cu toate acestea, acolo unde este posibil, facem referire şi la activitățile serviciilor secrete ale altor țări şi ne punem problema diferențelor dintre aceste servicii, diferențe determinate de natura regimurilor pe care acestea le servesc.

Prezenta carte nu dezvăluie cititorilor nici un fel de secrete sau "informații din interior", fie ele spectaculoase sau lipsite de interes. Sperăm să oferim, în schimb, elementele necesare înțelegerii domeniului în sine, precum şi multe picanterii care, fără îndoială, vor continua să-şi croiască drumul spre public.

Capitolul 1

CE ESTE ACTIVITATEA DE INFORMAȚII?

În domeniul general al ficțiunii şi în imaginația publică, domeniul informațiilor a fost foarte des asociat cu spionajul şi comportamentul fără scrupule, cu şantajul sexual al unei Mata Hari şi acțiunile "de capă şi spadă" ale lui James Bond. Deşi activitățile de acest tip ocupă o anumită poziție în domeniul informațiilor, întregul concept este mult mai extins. Pentru a surprinde această vastitate, putem începe prin analizarea diferitelor categorii de fenomene cărora li se aplică termenul "informații"; acestea includ anumite *informații*, *activități* şi *organizații*.[1]

> Domeniul informațiilor se referă la *informațiile* relevante pentru formularea şi implementarea unei politici guvernamentale în scopul promovării intereselor sale de securitate națională şi prevenirii amenințărilor din partea unor adversari existenți sau potențiali. (Termenul "adversar" este folosit aici într-un sens larg. De exemplu, o guvernare prietenoasă, cu care se negociază un tratat, poate fi *adversar în contextul negocierilor*; se presupune că părțile intră în competiție pentru a maximiza beneficiile pe care le obțin în urma acordului, cel puțin o parte pe cheltuiala celeilalte.) În cele mai clare şi mai importante dintre cazuri, aceste informații se referă la aspecte din domeniul militar, precum capacitatea adversarului şi planurile pentru o acțiune militară. Inamicii existenți sau potențiali, în general, îşi dau toată silința pentru a păstra secrete aceste informații. Desigur, alte tipuri de informații secrete pot fi la fel de importante – de exemplu, informațiile referitoare la activitățile şi intențiile diplomatice ale altei țări, precum şi activitățile acesteia în domeniul informațiilor.

Pe lângă datele de acest tip, cunoaşterea multor altor tipuri de informații referitoare la un adversar existent sau potențial poate fi folositoare, chiar dacă adversarul nu intenționează să le păstreze secrete. Acestea pot să includă activitățile de politică internă şi referitoare la progresul societății, precum şi statisticile economice şi demografice. Cât din aceste date sunt publicate depinde de natura regimului politic. Într-o societate democratică, sunt aproape întotdeauna accesibile publicului. Un sistem autoritar sau totalitar, pe de altă parte, deseori încearcă să ascundă orice informații referitoare la politica sa internă, situația economică sau tendințe sociale pe care un adversar le-ar considera utile. Indiferent cât de mult din informațiile publice ("din surse deschise") ar trebui, în sens strict, să fie considerate "informații secrete", în mod categoric trebuie să aibă loc un proces prin care să fie în mod sistematic disponibile pentru oficialii

guvernului într-o formă utilizabilă. Un serviciu de informații preia deseori această activitate.

Informațiile nu includ numai "materialul brut" cules prin metode de spionaj sau în alt mod, ci şi analize şi evaluări care se bazează pe ele. Acest rezultat, denumit şi "produs" informativ, are o importanță deosebită pentru factorii legislativi. Proporția în care acest produs informativ face posibilă prezentarea unei evaluări exhaustive a situației, bazându-se pe toate datele disponibile, atât publice, cât şi secrete, variază de la un serviciu de informații la altul.

Ca *activitate*, domeniul informațiilor implică culegerea şi analizarea informațiilor. De asemenea, include activitățile întreprinse pentru a proteja activitățile informative împotriva adversarilor, fie prin împiedicarea accesului lor la informații, fie prin inducerea lor în eroare cu privire la unele fapte şi semnificația acestora.

Domeniul informațiilor cuprinde o gamă largă de activități. De exemplu, există metode diverse de culegere a informațiilor, precum spionajul, fotografierea aeriană, interceptarea comunicațiilor şi cercetarea prin folosirea documentelor publice disponibile, programe de radio şi televiziune şi Internet. Există, de asemenea, tehnici diferite pentru analizarea informațiilor care au fost culese: unele dintre acestea pot fi similare metodelor pe care le folosesc ştiințele sociale, iar altele, precum decodarea mesajelor codificate, sunt caracteristice domeniului informațiilor. În mod similar, negarea informațiilor față de alții, implică diverse activități, unele dintre acestea fiind similare cu cele ale agenților de aplicare a legii, precum investigarea şi urmărirea agenților străini suspectați pentru a afla ce fel de activități desfăşoară aceştia. Altele sunt mai ezoterice, precum folosirea codificării pentru a proteja comunicațiile (deşi progresele recente înregistrate în domeniul tehnologiei informației au descoperit capacități de codificare care pot fi comercializate). De asemenea, există metode diferite de inducere în eroare a adversarilor, precum operațiuni "agent dublu" şi transmitere de mesaje false (aceasta înseamnă transmiterea unor mesaje de inducere în eroare care anticipează faptul că adversarul le va intercepta şi le va da crezare).

Datorită acestei varietăți de activități, pare dificil de găsit un punct comun care să le relaționeze. Toate acestea au legătură cu obținerea sau contestarea informațiilor. De aceea, culegerea de informații ca activitate poate fi definită drept componentă a luptei între adversari care folosesc în primul rând informațiile (spre deosebire, de exemplu, de competiția economică, manevrele sau negocierile diplomatice, sau amenințările sau folosirea forței militare).

În fine, termenul "informații" se referă, de asemenea, la o *organizație* care efectuează aceste activități. Una dintre principalele caracteristici ale unor astfel de organizații este confidențialitatea cu care trebuie coordonate aceste activități. Multe dintre metodele lor de operare, precum folosirea agenților sub acoperire sau a regulilor stricte privind accesul la informații, sunt rezultatul acestei solicitări. Deoarece agențiile de

informații sunt organizate pentru a îmbunătăți capacitatea de asigurare a confidențialității, acestora li se poate atribui, împreună cu funcțiile privind informațiile, responsabilitatea efectuării activităților secrete pentru a promova obiectivele de politică externă ale guvernelor lor mai direct.

O astfel de activitate, denumită "acțiune secretă" în terminologia din domeniul informațiilor în SUA, poate cuprinde de la aspecte banale, precum asigurarea în mod secret a unei colaborări cu un guvern străin prieten, până la aspecte spectaculoase, precum orchestrarea răsturnării acelora ostile. Ideea ca acestea să intre în atribuțiile aceloraşi organizații care culeg şi analizează informații a reprezentat un aspect controversat. Chiar dacă, din motive birocratice, organizațiilor de informații li se atribuie responsabilitatea pentru acțiunile secrete, va rămâne problema fundamentală – din punct de vedere teoretic şi practic – dacă acțiunea secretă ar trebui considerată ca făcând parte din domeniul informațiilor.

Delimitarea Domeniului

Deoarece nu numai guvernele, ci şi alte tipuri de organizații acționează într-un mediu caracterizat de competitivitate, conceptul de informații poate fi aplicat şi în cazul acestora. De exemplu, unii cercetători extind conceptul şi asupra corporațiilor de afaceri, considerând informațiile drept "informații organizate … desemnate să întrunească criteriile unice ale politicii unei întreprinderi"[2] În mod similar, se poate vorbi despre o activitate de culegere de informații în cadrul unui partid politic sau campanii în încercarea de a afla ce plănuieşte opoziția.

Aceste posibile extinderi ale termenului "informații" nu sunt discutate în acest volum, care se limitează la obiectivele tradiționale ale domeniului informațiilor – adică la informații şi activități relevante pentru problemele de securitate naționale ale guvernelor.

Dar chiar şi acceptând această limitare, obiectivul domeniului informațiilor rămâne neclar într-o anumită măsură, de vreme ce termenul "securitate națională" este el însuşi nedefinit. Sensul său de bază se referă la protejarea națiunii împotriva amenințărilor, în ultimă instanță militare, reprezentate de națiuni străine. Atunci când o națiune este invadată sau este pe punctul de a fi atacată, problemele sale de securitate se concentrează în mod clar asupra apărării sau prevenirii invadării şi securizării împotriva unor situații similare pe viitor. În perioade mai puțin periculoase, poate fi mai puțin clar ce națiuni străine, evenimente sau circumstanțe amenință securitatea națională şi de aceea solicită atenția agențiilor de informații ale țării respective.[3]

Problema se complică şi mai mult prin faptul că interesele de securitate națională şi a amenințărilor la adresa lor, nu pot fi independente de tipul de guvernare a țării (sau regim) şi punctele de vedere ideologice. Deşi susținătorii Realpolitik ar argumenta că interesele unei națiuni sunt determinate de factorii obiectivi ai sistemului internațional, vederile

ideologice şi în general de cultura politică a ţării influenţează modul în care un guvern le percepe.[4] De exemplu, caracterul ideologic al unui regim poate stabili dacă acesta consideră o anumită ţară străină drept o ameninţare. În special, puterile revoluţionare au păreri tipice despre ceea ce constituie o ameninţare la adresa securităţii naţionale.

Informaţiile interne

O zonă mai importantă în care natura regimului afectează obiectivul domeniului informaţiilor este reprezentată de "informaţiile interne". Orice guvern trebui să fie preocupat nu numai de ameninţările externe (precum invazia militară), ci şi de ameninţările împotriva capacităţii de guvernare sau chiar împotriva existenţei acesteia, care sunt provocate de indivizi sau grupuri din interiorul graniţelor. Astfel de ameninţări ar putea veni din partea unor grupuri care încearcă să răstoarne guvernul prin mijloace ilegale, prin folosirea violenţei pentru schimbarea politicii de guvernare sau prin excluderea din organismul politic a unor membri aparţinând unei anumite etnii, rase sau grup religios. Dar modul în care un guvern defineşte astfel de ameninţări interne, depinde în mare măsură de tipul de guvernare care există.

Un regim în care o dinastie sau un singur partid politic deţin monopolul asupra puterii, de exemplu, probabil consideră orice disensiune internă politică drept o ameninţare a securităţii, iar serviciul de informaţii se va concentra asupra detectării şi îndepărtării acelei disensiuni. În cazuri extreme, guvernul unui stat totalitar poate considera toate persoanele care nu fac parte din partidul de guvernare drept actuali sau potenţiali duşmani.[5] Spre deosebire de aceasta, noţiunea de "oponenţi loiali", care se regăseşte în sistemele parlamentare sau alte sisteme democratice, implică faptul că oponenţii politici pe plan intern ai guvernului nu reprezintă ameninţări de securitate şi de aceea nu sunt ţinte pentru culegerea de informaţii.

În plus, grupările interne care sunt ostile nu numai guvernului în funcţie, ci şi sistemului fundamental de guvernare al naţiunii (sau regimului) pot intra în relaţii cu puteri străine în diferite moduri. La un capăt al spectrului extern-intern va fi un individ sau un grup care acţionează în numele, şi în direcţia unei puteri străine ostile. Ar putea exista, de asemenea, grupuri sau indivizi care împărtăşesc obiective comune cu o putere străină şi să coopereze pentru realizarea scopurilor lor. Ar putea exista grupări care împărtăşesc convingeri ideologice sau de altă natură cu un adversar străin dar care nu au practic legături cu acesta. Regimuri diferite pot avea păreri diverse cu privire la tipul de grupare care reprezintă o ameninţare la adresa securităţii naţionale, împotriva căreia trebuie culese informaţii.

Activitatea de informaţii şi aplicarea legii

O problemă asociată este reprezentată de ameninţările denumite "transnaţionale", care nu sunt generate în primul rând de un guvern străin – de exemplu, traficul de narcotice, terorismul internaţional sau anumite tipuri

de crimă organizată. Acestea pot reprezenta ameninţări serioase la adresa bunăstării unei naţiuni, dar sunt mai degrabă responsabilitatea agenţiilor de aplicare a legii, nu a serviciilor de informaţii. Oricum, serviciile de informaţii sunt adesea implicate în lupta împotriva lor, din mai multe motive. În primul rând, acestea implică activităţi în ţări străine, unde agenţiile de aplicare a legii dintr-un anumit stat nu sunt abilitate să acţioneze, iar agenţiile de aplicarea a legii din ţările respective nu sunt capabile, sau nu doresc să ofere asistenţă. Serviciile de informaţii pot fi solicitate pentru informaţii referitoare la caracteristicile externe ale acestor activităţi, informaţii care nu ar putea fi disponibile în alt mod.

În al doilea rând, implicarea agenţiilor de aplicare a legii presupune de obicei aşteptarea până când o infracţiune a fost sau este pe punctul de a fi săvârşită şi de abia atunci se încearcă rezolvarea cazului respectiv, precum şi arestarea infractorilor. Aceasta ar putea să nu fie o abordare adecvată în ceea ce priveşte anumite ameninţări transnaţionale. Un singur incident, precum aruncarea în aer a unui avion de pasageri în timpul zborului, poate cauza pagube atât de mari, încât un guvern trebuie să încerce prevenirea unui astfel de incident şi nu rezolvarea acestuia după ce s-a produs. Mai mult decât atât, o anumită infracţiune, cum ar fi un simplu caz de contrabandă cu narcotice, poate fi doar o parte din cadrul unor operaţiuni ale unei organizaţii criminale; dacă este o organizaţie mare şi bine organizată, arestarea unor infractori care au comis o singură infracţiune poate să nu aibă un impact prea puternic. Astfel de arestări ocazionale pot reprezenta, din perspectiva liderilor, un preţ acceptabil pentru derularea afacerii. Chiar dacă agenţiile se mulţumesc să aştepte până când se comite o anumită infracţiune, şansele de rezolvare depind foarte mult de informaţiile disponibile referitoare la organizaţia implicată.

Din aceste motive, guvernele adoptă adesea o abordare informativă specifică acestor tipuri de activitate. În loc să aştepte comiterea unei anumite infracţiuni asupra căreia să se concentreze, agenţiile adună informaţii pe timp îndelungat cu privire la anumiţi indivizii şi grupări – motivaţiile lor, resursele, interconexiunile, intenţiile şi aşa mai departe. Se impune adesea folosirea unor informatori, care se infiltrează în grupările implicate şi operează asemenea spionilor. Este posibil, de asemenea, să se intercepteze comunicaţiile sau să se folosească alte metode tehnice pentru culegerea de informaţii. De aceea, agenţiile de informaţii sunt deseori implicate în lupta împotriva grupărilor transnaţionale. În funcţie de regim, implicarea agenţiilor poate fi limitată la caracteristicile externe ale activităţilor lor, în timp ce aspectele interne rămân în atribuţiile agenţiilor de aplicare a legii.

Chiar şi în abordarea problemei reprezentate de grupările de criminalitate organizată care acţionează în totalitate pe plan intern, agenţiile de aplicare a legii folosesc adesea tehnici specifice culegerii de informaţii. De exemplu, în ceea ce priveşte menţinerea legii pe plan intern, Biroul Federal de Investigaţii SUA (FBI) face distincţia între anchetele penale secrete şi anchetele penale obişnuite. Dintre acestea două, primul tip de investigaţii este descris ca "mai extins şi mai puţin discriminator decât cel obişnuit"; acesta nu

se concentrează asupra săvârşirii unei singure acţiuni infracţionale, ci asupra unei organizaţii criminale, fiind necesară stabilirea dimensiunii şi structurii acesteia, a acţiunilor sale trecute, a intenţiilor criminale şi a capacităţii de a produce pagube.[7] Diferenţa între abordarea agenţiilor de aplicare legii şi a serviciilor de informaţii este reprezentată de atenţia care poate fi îndreptată fie către pedepsirea unei anumite acţiuni criminale, fie către lupta cu o organizaţie implicată într-o activitate criminală.

Economia şi activitatea de informaţii

Există întrebări referitoare la modul de funcţionare al agenţiilor de informaţii în ceea ce priveşte problemele economice. Din nou, multe depind de natura regimului şi de sistemul economic al ţării. Într-un sistem cu economie coordonată de guvern, domeniul informaţiilor se va concentra asupra aspectelor economice privind relaţiile guvernului respectiv cu guverne străine (precum comerţul internaţional) în aceeaşi măsură ca şi toate celelalte aspecte de relaţii internaţionale. În plus, informaţiile pot fi folosite pentru consolidarea situaţiei economice a statului. Achiziţionarea tehnologiei occidentale avansate, de exemplu, a reprezentat o sarcină importantă a serviciilor de informaţii ale Uniunii Sovietice (şi rămâne un obiectiv important al serviciilor de informaţii rus şi chinez). Această activitate nu numai că a ridicat nivelul tehnologic al armatei sovietice sau chineze, dar a şi scutit ambele ţări de cheltuieli ridicate şi de dificultatea de a dezvolta o tehnologie proprie, fie în scop militar, fie civil.[8]

Într-o economie de piaţă, nu este foarte clar care sunt aspectele economice importante pentru securitatea naţională care justifică sau presupun implicarea agenţiilor de informaţii. Există un număr de domenii specifice, precum evaluarea capacităţii economice a unui potenţial adversar militar sau progresele ulterioare care afectează fluxul de resurse vitale strategice, asupra cărora guvernele pot cere informaţii detaliate. Angajarea agenţiilor şi folosirea metodelor de culegere a informaţiilor depinde într-o oarecare măsură de încercarea statelor respective de a le păstra sau nu secrete. În general, problemele specifice economice cu impact direct asupra aspectelor de securitate naţională care privesc politica militară sau externă intră în responsabilitatea agenţiilor de informaţii. De exemplu, pe timp de război, metodele activităţii de informaţii pot fi folosite pentru a obţine acces la materiale strategice (sau pentru a induce în eroare adversarii astfel încât să nu aibă acces la acestea), un obiectiv cheie al securităţii naţionale. În mod similar, în decursul negocierilor cu o ţară străină pe probleme economice, o naţiune îşi poate folosi resursele secrete pentru a afla care sunt avantajele partenerului în urma negocierilor.

Interesul manifestat de un stat cu privire la informaţiile de natură economică legate de activitatea industrială, comercială sau financiară ale altor state depinde probabil de faptul că guvernul acesteia are o autoritate de "strategie industrială" care poate folosi aceste informaţii. Ca urmare, problema legată de folosirea agenţiilor de informaţii pentru a culege

informații economice reprezintă într-o mare măsură surogate pentru o dezbatere fundamentală privind rolul guvernului în direcționarea viitorului economic al țării.

De asemenea, se dezbate intens pe tema folosirii metodelor informative pentru dezvoltarea situației economice a unei națiuni[9]. Deoarece încheierea Războiului Rece a redus riscul unei confruntări militare între principalele puteri, puterea economică a început să câştiga o poziție importantă în stabilirea puterii şi a prestigiului internațional al unei țări; în consecință, a apărut un interes crescut pentru rolul pe care informațiile îl puteau juca în consolidarea situației economice.[10] Situația economică a unei națiuni se îmbunătățeşte sau se degradează în timp din cauza unor factori precum coeficientul de investiții, productivitatea muncii, aptitudinile de management şi nivelul educației forței de muncă. În plus, deşi multe progrese din economia internațională pot avea importante consecințe pentru securitatea națională, nu este clar dacă guvernul ar trebui sau dacă ar putea face prea multe în privința acestor progrese. Mai mult decât atât, într-o societate democratică, politica economică pare a fi mai degrabă determinată de interacțiunile intereselor economice pe plan intern decât de orice viziune coerentă (bazată sau nu pe informații) a unei viitoare situații economice mondiale. Din aceste motive, nu este clar dacă un guvern precum cel al Statelor Unite ar fi un consumator important al unor astfel de informații. Acestea ar putea servi interesele economice, dar nu este clar dacă informațiile culese clandestin pe cheltuiala guvernului ar putea fi distribuite echitabil unor indivizi sau corporații pentru interese private ulterioare.[11]

Alte aspecte "non-tradiționale"

Unii absolvenți din domeniul informațiilor au afirmat că pe lângă aspectele economice mai există şi preocupări "non-tradiționale" care trebuie luate în considerare în domeniul culegerii de informații – de exemplu, probleme referitoare la mediu. Deşi există argumente conform cărora problemele de mediu pot afecta securitatea națională, motivul principal pare a fi acela că sistemele tehnice de culegere de informații dezvoltate în alte scopuri pot ajuta la urmărirea schimbărilor de mediu de-a lungul timpului şi pe zone extinse şi că pot face aceasta prin costuri suplimentare scăzute.[12]

SERVICIILE SECRETE ÎN ERA INFORMAȚIILOR

Ținând cont de faptul că serviciile secrete lucrează cu informații, este corect să presupunem că va fi afectat în mod serios de apariția a ceea ce a fost denumită "era informațiilor". Noțiunea de eră a informațiilor este destul de ambiguă. Totuşi, în mod clar este foarte importantă; deja a schimbat modul în care multe organizații operează – în special corporațiile din domeniul afacerilor – şi probabil va avea efecte importante asupra guvernului.

Din punct de vedere tehnic, factorul coordonator este progresul tehnologic extraordinar care s-a înregistrat în procesarea şi comunicarea informaţiilor. Schimbarea tehnologică reprezintă doar o mică parte a întregii imagini: mai importante sunt schimbările de comportament şi instituţionale care rezultă în urma concentrării asupra informaţiilor care reprezintă cheia activităţii organizaţionale. (În domeniul militar, ceea ce este adesea denumit "revoluţia în afacerile militare" depinde foarte mult de utilitatea sporită a informaţiilor prin selectarea unor noi tipuri de arme de precizie şi prin întărirea capacităţii de a culege, procesa şi disemina acele informaţii într-un timp scurt în scop operaţional.)

Efectul acestor schimbări este resimţit în diverse forme. Pe de o parte, acestea sugerează noi moduri în care informaţiile pot fi transferate mai rapid şi folosite în interiorul guvernului, astfel încât formularea şi implementarea politicii să fie mai eficiente. În plus, acestea se concentrează asupra unei cantităţi sporite de informaţii disponibile pentru întreaga societate, la nivelul unor departamente ale guvernului care nu fac parte din serviciile de informaţii şi, de asemenea, în afara guvernului. Cu alte cuvinte, serviciile de informaţii consideră că alte tipuri de organizaţii devin mai eficiente pentru culegerea, analizarea şi transmiterea informaţiilor – aceasta înseamnă că serviciile de informaţii au, în ceea ce priveşte unele tipuri de informaţii, o "concurenţă" mai mare în furnizarea informaţiilor pentru factorii de decizie. Din perspectiva guvernului, este important să se găsească o modalitate cât mai eficientă de exploatare a informaţiilor generate şi transmise oriunde în societate precum şi să se asigure că produsul unic al serviciilor de informaţii este combinat cu alte surse de informaţii într-un mod care să întrunească cel mai bine nevoia de informaţii a guvernului.[13]

ELEMETELE CULEGERII DE INFORMAŢII

Indiferent de raza de acţiune, în funcţie de tipul activităţii implicate, informaţiile pot fi clasificate în patru categorii, la care se face referire de obicei ca fiind "componente ale domeniului informaţiilor": culegerea, analiza, acţiuni secrete şi contra-informaţiile. Deoarece aceste elemente sunt analizate în detaliu în următoarele capitole, discuţia care urmează îşi propune doar să elucideze natura celor patru tipuri de activităţi de informaţii şi să schiţeze relaţiile dintre acestea.

Culegerea se referă la adunarea datelor brute, prin spionaj; metode tehnice (fotografie, interceptarea comunicaţiilor electronice şi alte metode care implică tehnologia); exploatarea "surselor deschise" (de exemplu, publicaţiile, emisiunile de radio şi televiziune); sau prin orice alte metode. În timp ce culegerea este în mod clar fundamentală activităţii de informaţii, există opinii diferite în ceea ce priveşte importanţa relativă a diferitelor metode. De exemplu, absolvenţii din domeniul informaţiilor au dezbătut importanţa relativă a culegerii din "surse deschise" comparativ cu metodele

unice ale serviciilor de informaţii precum şi importanţa relativă a spionajului comparativ cu culegerea prin mijloace tehnice.

Indiferent cât de bune sunt informaţiile culese, aproape niciodată nu vorbesc pentru ele însele. Cu alte cuvinte, unele analize de informaţii sunt necesare pentru a fi de folos factorilor de decizie şi comandanţilor militari. În marea majoritate a cazurilor, informaţiile culese sunt fragmentare, ambigue şi susceptibile de interpretări divergente. De aceea, procesul analizării informaţiilor disponibile pentru a emite judecăţi referitoare la capacităţile, intenţiile şi acţiunile unei alte părţi reprezintă o componentă vitală a procesului de informaţii. Chiar mai dificil este procesul de anticipare ("estimare" în jargonul de informaţii american) a capacităţilor viitoare, intenţiilor şi acţiunilor unui guvern străin sau ale unei organizaţii politice.

În plan conceptual, acţiunea sub acoperire diferă de alte componente ale domeniului informaţiilor în sensul că, în timp ce altele se concentrează asupra căutării şi protejării informaţiilor, acţiunile sub acoperire urmăresc să influenţeze în mod direct evenimentele politice. În ceea ce priveşte intensitatea, acţiunea sub acoperire poate varia de la persuasiune sau propagandă la acţiune paramilitară; a fost descrisă ca "o activitate la limita dintre diplomaţie şi război."[14]

Deşi tehnicile pentru exercitarea influenţei sunt numeroase, ele au o particularitate comună de anonimat – rolul guvernului în coordonarea activităţii nu este aparent sau nu este cunoscut public. Din acest motiv, capacitatea unei agenţii de informaţii de a acţiona în secret, presupune de cele mai multe ori că poate derula şi acţiuni secrete. Dar, după cum am afirmat mai sus, deoarece această activitate implică mai degrabă implementarea unei strategii decât informarea factorilor de decizie, în Statele Unite s-a sugerat de multe ori ca acţiunile secrete să nu fie derulate de aceeaşi agenţie (adică Agenţia Centrală de Informaţii) care culege şi analizează informaţiile secrete. Pe de altă parte, atât în Statele Unite, cât şi în Marea Britanie s-a descoperit din experienţele anterioare că având două agenţii care coordonează operaţiuni clandestine (una pentru spionaj şi cealaltă pentru acţiuni sub acoperire) se poate ajunge la o rivalitate epuizantă, dublarea efortului şi interferenţă reciprocă.[15]

În sensul cel mai general, contra-informaţiile caută să protejeze societatea (şi în special capacităţile din domeniul informaţiilor) împotriva oricăror ameninţări care pot fi cauzate de servicii de informaţii ostile. În primul rând, contra-informaţiile implică inducerea în eroare a adversarilor. Această protecţie este realizată prin programe de securitate (acţiuni întreprinse pentru a reţine informaţiile departe de cei care nu sunt autorizaţi pentru a le primi); şi prin contraspionaj (acţiuni întreprinse pentru a reţine sau neutraliza agenţii străini, astfel încât să se prevină obţinerea şi comunicarea de către aceştia a informaţiilor secrete). În plus, activitatea de contra-informaţii poate avea rolul de a proteja împotriva capacităţii adversarului de a culege informaţii şi de a le analiza; aceasta se realizează prin operaţiuni de dezinformare care furnizează concluzii false sau

intenționat eronate pentru a induce adversarului ajungerea la concluzii incorecte cu privire la capacitățile, acțiunile sau intențiile cuiva.

Protejarea împotriva capacităților de informații ale unui adversar, în sensul larg, presupune, de asemenea, şi alte activități. Poate fi necesar să se parcurgă anumite etape pentru a evita dezinformarea prin informații eronate furnizate deliberat de către cealaltă parte. De aceea, contra-informațiile trebuie să protejeze integritatea funcțiilor de culegere şi analiză. De asemenea, este important să se cunoască acțiunile secrete întreprinse de un guvern străin pentru a influența guvernul sau societatea unei țări. În ultimul rând, extinderea activităților de contra-informații este determinată de amenințarea reprezentată de activitățile de informații ale adversarului.

Capitolul 2

SPIONI, MAŞINI ŞI BIBLIOTECI: CULEGEREA DE INFORMAŢII

Începem discuţia privind elementele activităţii de informaţii prin analizarea culegerii informaţiilor brute care, odată corelate şi analizate, formează baza judecăţilor şi evaluărilor din domeniul informaţiilor. Diversele metode de culegere ("disciplinele" domeniului informaţiilor) pot fi clasificate astfel: (1) culegerea din surse umane (la care se face referire ca spionaj, culegere de informaţii din surse umane sau în jargonul domeniului de informaţii din SUA, humint), (2) culegerea prin metode tehnice (informaţii tehnice sau technit) şi (3) culegerea nesecretă prin contacte diplomatice sau din surse de informaţii general disponibile, precum ziarele, Website-ul sau alte resurse bazate pe Internet şi emisiuni de radio şi televiziune (culegerea din surse deschise).[1]

CULEGEREA DE INFORMAŢII DIN SURSE UMANE

Culegerea de informaţii din surse umane sau spionajul reprezintă prima semnificaţie a termenului "informaţii" care îi vine cuiva în minte. Acesta implică identificarea şi recrutarea unui oficial străin care, prin virtutea poziţiei de încredere pe care o ocupă în guvern, are acces la informaţii valoroase şi care doreşte, din anumite motive, să le transmită ofiţerilor unui serviciu de informaţii. În unele cazuri (în special în timp de război), persoana care furnizează informaţiile poate să nu fie un oficial guvernamental, ci o persoană privată care are ocazia să observe (sau să audă despre) aspecte de interes, precum sosirea sau plecarea unor nave dintr-un port. Persoana care este recrutată poate fi, de asemenea, cineva care are acces la informaţii importante în virtutea unei relaţii apropiate (prietenie, afaceri, etc.) cu cineva de interes pentru domeniul informaţiilor (de exemplu, un terorist sau un traficant internaţional de arme).

În mod obişnuit, sunt implicate persoane cu două roluri diferite: un *ofiţer de informaţii*, angajat al unei agenţii de informaţii şi o *sursă*, care îi furnizează ofiţerului informaţii pentru a fi transmise conducerii serviciului de informaţii. Ofiţerul de informaţii sau "dirijorul" păstrează legătura cu sursa, transmite instrucţiunile primite de la superiori, asigură resursele necesare (precum echipamentele de copiere sau comunicaţii) şi, în general, încearcă să asigure continuitatea fluxului de informaţii .[2]

Tipuri de ofițeri de informații

Deoarece ofițerii de informații nu trebuie să atragă atenția guvernului din țara în care operează, aceştia nu îşi pot declara public intenția de a oferi bani în schimbul unor informații secrete. Aceştia trebuie să aibă ceea ce în jargonul domeniului informațiilor se numeşte "acoperire" – adică un motiv plauzibil pentru a se afla în acea țară, metode vizibile de susținere financiară, un pretext pentru a se întâlni cu persoane care au acces la informații de importanță deosebită şi aşa mai departe.[3]

În limbajul actual din SUA, se face diferența între acoperire "oficială" şi "neoficială". Acoperirea oficială se referă la deghizarea unui ofițer de informații în diplomat sau într-un alt tip de funcționar guvernamental care este trimis la post în străinătate. Acoperirea neoficială se referă la orice alt tip de deghizare – ca om de afaceri, jurnalist, turist, etc. – ceea ce ar putea explica de ce un ofițer se află în țara respectivă. Un agent sub acoperire neoficială îşi poate ascunde, de asemenea, naționalitatea pretinzând a fi dintr-o altă țară decât aceea a cărui ofițer de informații este în realitate.[4] Dacă țara gazdă este una care de obicei acceptă imigranți, ofițerul poate intra sub acea acoperire.

Folosirea unei acoperiri oficiale are mai multe avantaje. În mod clar, îi poate oferi ofițerului de informații imunitate diplomatică. Dacă activitățile sale de spionaj sunt detectate, legea internațională delimitează strict condițiile în care guvernul gazdă îl poate declara *persona non grata* şi expulza din țară.

În plus, statutul de diplomat asigură accesul ofițerului de informații la anumite surse; în calitate de diplomat, acesta ar putea, fără a ridica suspiciuni, să se întâlnească cu oficiali guvernamentali ai țării gazdă în cadrul activității sale obişnuite, precum şi cu alți diplomați aflați la post în aceeaşi capitală. Dacă şi alte țări vor folosi, de asemenea, o acoperire oficială pentru ofițerii lor de informații, va avea ocazii "nevinovate" pentru a se întâlni cu aceştia.[5]

De asemenea, trimiterea la post a unor agenți de informații într-o ambasadă sub acoperire oficială garantează că, în cazul în care un cetățean al țării gazdă abordează ambasada în legătură cu anumite materiale confidențiale sau cu o ofertă pentru a le furniza, problema poate fi rezolvată de un profesionist în domeniul informațiilor. În acest sens, existența unor ofițeri de informații cu acoperire oficială facilitează încercarea țării-gazdă de a contacta serviciul de informații; astfel de posturi sunt folosite drept "căsuțe poştale" pe cât de utile, pe atât de necesare, în special în țările care reglementează strict sau interzic cetățenilor călătoriile sau comunicațiile cu lumea exterioară.[6]

Acoperirea oficială presupune, de asemenea, avantaje administrative. Ofițerul poate fi plătit şi se pot rezolva alte probleme legate de personal prin canalele guvernamentale obişnuite, iar comunicațiile securizate cu serviciul de informații pot fi asigurate prin "stația" de informații (grupul de ofițeri de informații sub acoperire oficială).[7]

În acelaşi timp, acoperirea oficială are şi câteva inconveniente. Cel mai important, datorită numărului relativ redus de oficiali trimişi la post într-o anumită ţară gazdă, serviciul de informaţii al ţării respective poate avea capacitatea de a stabili, destul de precis, care dintre "diplomaţi" sunt ofiţeri de informaţii şi care nu. Acest lucru se poate realiza prin metode clare, dar laborioase, de menţinere a supravegherii asupra fiecărui oficial şi prin observarea deplasărilor, a contactelor, prin interceptarea telefoanelor, instalarea de echipamente de interceptare în apartamente şi aşa mai departe. Practica angajării cetăţenilor din ţara gazdă pentru a lucra în interiorul ambasadelor în anumite posturi facilitează o astfel de supraveghere, în special în acele ţări unde se presupune că oricine căruia i se permite să lucreze într-o ambasadă străină a fost de acord să coopereze cu serviciul de informaţii al ţării gazdă.[8] În plus, se poate ajunge la acelaşi rezultat prin metode mai simple şi mai puţin costisitoare. De exemplu, materialele publicate de o anumită ţară ar putea fi folosite pentru a urmări cariera ofiţerilor săi de servicii externe şi a identifica astfel caracteristicile care indică o legătură cu serviciile de informaţii.

Mai mult decât atât, deşi acoperirea oficială poate asigura accesul facil la potenţialele surse (în primul rând alţi diplomaţi şi oficiali din serviciile secrete ale ţării gazdă), ea poate obstrucţiona accesul la alte persoane care ar putea ezita să intre în contact cu oficiali străini, în general, sau cu aceia dintr-o anumită ţară. În oricare dintre cazuri, potenţialii recruţi sunt atenţionaţi că intră în contact cu un oficial al unui guvern străin şi astfel devin mai precauţi. În plus, dacă relaţiile diplomatice se deteriorează, cum se poate întâmpla în cazul unei crize puternice sau al unui război – când este vital să se obţină informaţii de calitate – ofiţerii sub acoperire oficială părăsesc ţara, prin aceasta întrerupându-se activitatea oricărei reţele de surse pe care ar fi putut-o crea.[9]

Avantajele şi dezavantajele unei acoperiri neoficiale sunt, în cea mai mare parte, opusul celor deja discutate. Pe de o parte, de vreme ce aceştia pretind a avea diverse profesii şi statute sociale, oficialii fără acoperire oficială (NOC) pot avea acces la diferite surse din diverse medii. În mod similar, aceştia pot pretinde că sunt (sau chiar să fie) fie cetăţeni ai ţării unde sunt trimişi, fie ai unei terţe ţări. Ascunderea legăturii cu guvernul pentru care lucrează îi poate ajuta să intre în contact cu potenţialele surse şi să obţină accesul la informaţii. Dacă relaţiile diplomatice sunt întrerupte, aceştia pot rămâne şi continua operaţiunea. În general, NOC sunt mai greu de identificat de către guvernul gazdă.

Pe de altă parte, acoperirea neoficială presupune multe dezavantaje. Cheltuielile şi dificultăţile administrative în asigurarea acoperirii neoficiale sunt mai mari decât în cazul acoperirii oficiale. Una dintre metode este convingerea unei corporaţii sau altei organizaţii private să permită unui ofiţer de informaţii să fie angajat ca membru în personalul său. O altă soluţie ar fi ca ofiţerii pot să pună bazele unei afaceri sau să se implice în alte activităţi care să justifice prezenţa lor în ţara ţintă. Însă această metodă nu numai că implică cheltuieli majore, dar şi un efort de durată din partea

ofițerului de informații pentru a crea o acoperire convingătoare a activității sale, ceea ce ar reduce timpul şi efortul pe care ofițerul le-ar putea dedica activității sale principale de culegere de informații.[10] Comunicațiile pot fi mai dificile, din moment ce NOC nu poate folosi în mod regulat serviciile de comunicații ale ambasadei fără a trezi suspiciuni. Un binecunoscut NOC a fost Richard Sorge, un cetățean german, corespondent al unui important ziar din Germania, care a spionat pentru serviciul militar de informații sovietic în China şi Japonia din anii 1930 până în toamna lui 1941, când a fost arestat. Relațiile sale apropiate cu personalul ambasadei germane din Tokio, inclusiv cu ambasadorul, i-au asigurat accesul la informații privind planurile de război ale Germaniei şi Japoniei. Cu puțin timp înainte să fie arestat, Sorge a raportat Moscovei informații de mare gravitate referitoare la faptul că "Estul îndepărtat al Uniunii Sovietice poate fi considerat la adăpost de atacurile japoneze." Conform raportului lui Sorge, Japonia hotărâse să nu atace Uniunea Sovietică; în schimb, urma să declanşeze atacuri împotriva Statelor Unite în sudul şi estul Pacificului, precum şi împotriva coloniilor britanice şi germane din Asia de sud-est. Stalin a transferat liniştit sute de mii de trupe din Estul îndepărtat la Moscova, unde ar fi urmat să stopeze avansarea Germaniei în iarna 1941-42. Privind retrospectiv, oprirea înaintării trupelor germane în afara Moscovei a reprezentat un moment de cotitură în desfăşurarea războiului.[11]

Un alt exemplu al folosirii cu succes a unei acoperiri neoficiale, un exemplu care ilustrează valoarea capacității de deghizare a naționalității, este acela al unui agent israelian, Eli Cohen. Evreu de naționalitate egipteană, Cohen a emigrat în Israel în 1956 la vârsta de treizeci şi doi de ani şi s-a oferit ca voluntar pentru serviciul de informații israelian. A fost trimis de agenția israeliană de informații, Mossad, în Argentina în 1961 pentru a-şi construi o acoperire ca om de afaceri musulman, sub pseudonimul Kamal Amin Taabet. După ce şi-a stabilit cu rapiditate un număr mare de contacte în comunitatea sirienilor expatriați din Argentina, Cohen s-a mutat la Damasc la începutul anului 1962. Înarmat cu scrisori de recomandare furnizate de noii săi prieteni sirieni din Buenos Aires, Cohen a reuşit (cu ceva noroc) să pătrundă în cercurile înalte din Siria. De fapt, avea relații atât de puternice, încât la un moment dat, a fost folosit ca emisar între noul guvern Baath şi un fost preşedinte exilat al Siriei; altă dată, a fost propus pentru un post în cabinetul guvernului sirian. După ce a raportat timp de trei ani despre problemele de ordin politic, militar şi diplomatic, Cohen a fost prins de serviciul de contraspionaj sirian şi executat în mai 1965.[12]

O utilizare ambițioasă a acoperirii neoficiale implică ofițerii care pătrund în țări străine deghizați ca imigranți obişnuiți. În mod clar, este mai uşor să introduci astfel de ofițeri într-o țară care primeşte în mod obişnuit un număr mare de imigranți şi vizitatori şi care foloseşte metode relativ neatente de control al granițelor, decât într-o țară care nu primeşte imigranți şi în general supraveghează strict vizitatorii şi îşi păzeşte cu atenție granițele.

Un exemplu interesant care ilustrează cât timp şi efort era dispusă Uniunea Sovietică să acorde operațiunilor de acest tip este acela al lui Ludek

Zemenel, un cetățean ceh recrutat de serviciul de informații sovietic (Comisia de Securitate a Statului, cunoscută sub numele de KGB de la inițialele sale în limba rusă).[13] Folosind identitatea unui anume Rudolf Herrman (adevăratul Rudolf Herrman era un german care murise în Uniunea Sovietică în timpul celui de al doilea război mondial), el a trăit în Germania Democrată timp de un an. Apoi, la sfârşitul anului 1957, a plecat împreună cu soția sa est germană (de asemenea, ofițer de informații sovietic) şi un fiu minor în Germania Federală, unde părea a fi un refugiat obişnuit est german.[14]

După patru ani în Germania de Vest, Herrmann a emigrat în Canada, unde şi-a deschis o mică afacere, realizând filme publicitare şi comerciale. El a îndeplinit o serie de misiuni minore pentru KGB, cum ar fi întocmirea unor "rapoarte de personalitate" privind politicienii şi jurnaliştii pe care i-a întâlnit prin intermediul afacerii sale şi menținerea relațiilor cu un profesor canadian, care era agent KGB. Totuşi, cea mai importantă misiune a sa a fost ascunderea calității sale pentru a putea prelua controlul asupra rețelei de surse canadiene de la "rezidentul" legal (şeful bazei KGB de la ambasada sovietică din Ottawa), în cazul unei rupturi în relațiile diplomatice dintre Canada şi URSS.

După şase ani petrecuți în Canada, lui Herrmann i s-a cerut să se mute din Canada în Statele Unite, unde a îndeplinit misiuni similare. Când fiul său Peter a împlinit vârsta de 17 ani, Herrmann l-a recrutat şi pe acesta pentru a lucra în KGB. Întrucât Peter fusese adus de mic în Germania de Vest şi fusese crescut de la vârsta de 4 ani în Canada şi Statele Unite, trecutul său nu avea motive să provoace suspiciuni; acesta avea să se pregătească pentru o carieră în guvernul american, unde putea opera ca sursă sovietică pe termen lung, sau ca o "cârtiță". Se pare că ar fi putut să facă acest lucru dacă FBI nu ar fi obținut acceptul de cooperare din partea tatălui său, în urma lansării unor amenințări cu închisoarea la adresa acestuia, a soției şi fiului.

Combinația de agenți sub acoperire oficiali sau neoficiali, pe care guvernul îi angajează pentru a executa activități de recrutare depinde de mai mulți factori. În general vorbind, cele mai importante sunt tipul de informații căutate şi modalitățile disponibile în vederea obținerii acestora. În cazul Statelor Unite şi aliaților săi, în perioada Războiului Rece, recrutarea de personal împotriva Uniunii Sovietice s-a axat în principal pe intențiile conducerii sovietice, capacitățile militare ale națiunii şi eforturile depuse de serviciile de informații împotriva Occidentului. Acest aspect, alături de monitorizarea atentă a tuturor cetățenilor străini de către serviciile sovietice de securitate, însemna că eforturile de recrutare de personal ale Statelor Unite şi ale altor țări s-au bazat în principal pe ofițeri de securitate care acționau sub acoperire oficială.

Pe de altă parte, de curând, China a folosit în special ofițeri sub acoperire neoficială pentru a-şi desfăşura programul de recrutare în Statele Unite; aceasta, în ciuda faptului că serviciile de informații chineze efectuează, într-adevăr, activități obişnuite de recrutare şi culegere prin

utilizarea unor metode sub acoperire, inclusiv a unor companii de fațadă, programe ştiințifice şi de schimb de experiență între studenți, precum şi delegații comerciale şi ştiințifice. De asemenea, serviciile de informații chineze utilizează agenți "inactivi" pe termen lung, care emigrează din China şi se stabilesc ca rezidenți pe o perioadă îndelungată înainte de a desfăşura activități secrete în țările în care au emigrat. Utilizarea excesivă a agenților sub acoperire neoficiali decurge din prioritatea pe care guvernul chinez a acordat-o achiziționării de tehnologie şi informații americane avansate, din natura relativ deschisă a pieței comerciale americane, din uşurința cu care se poate obține drept de reşedință în Statele Unite şi din existența unei comunități extinse de cetățeni chinezi în Statele Unite, printre care se pot amesteca emigranții nou-veniți.[15]

Tipuri de surse de informații

Aşa cum putem clasifica ofițerii de securitate ca fiind sub acoperire oficială sau neoficială, putem face o diferențiere între mai multe tipuri de surse de informații. Una dintre diferențele de bază este aceea dintre sursele pe care un ofițer de securitate, după ce pregăteşte terenul, le recrutează în mod activ în slujba agenției de securitate şi *voluntari*, care se oferă din proprie inițiativă să ajute agenția de securitate a unei țări străine, uneori apelând direct la ambasada respectivei țări.

Sursele recrutate sunt privite de obicei cu mai multă încredere, întrucât ofițerul de securitate a avut ocazia de a le studia caracterul şi motivația înainte de a le recruta.[16] În plus, sursele ce urmează a fi recrutate vor fi alese în funcție de nivelul lor de acces la informații importante. Cu toate acestea, identificarea şi recrutarea surselor presupune un efort laborios şi îndelungat, şi nu există garanții că până şi cea mai atent aleasă şi studiată sursă va răspunde pozitiv la încercările de recrutare sau "agățare".

Pe de altă parte, există oricum o suspiciune care planează asupra voluntarilor întrucât există întotdeauna posibilitatea ca un presupus voluntar să fi fost în realitate dislocat de serviciul de informații al propriei țări pentru a oferi informații false şi înşelătoare, pentru a-şi informa țara cu privire la metodele de operare ale serviciilor adverse sau pentru a întinde o cursă unuia dintre ofițerii serviciului advers în vederea arestării sau expulzării acestuia. Cu toate acestea, un serviciu de informații care are suspiciuni prea mari în privința voluntarilor poate rata ocazia de a obține informații la care ar fi putut avea acces cu uşurință. În trecutul serviciilor de informații există relatări legate de voluntari care au fost inițial ignorați sau refuzați, dar care au sfârşit prin a reprezenta surse valoroase pentru acestea.

Un caz faimos de acest gen l-a avut ca protagonist pe Fritz Kolbe, un reprezentant al ministerului german de Externe, în timpul Războiului Rece. Misiunea lui Kolbe presupunea selectarea informațiilor trimise zilnic prin telegraf la Berlin de toate ambasadele germane din întreaga lume. Informațiile priveau de obicei teme delicate referitoare la probleme strategice, militare şi secrete, precum şi diplomatice. După ce a reuşit să

obţină postul de curier oficial ocazional, în august 1943, Kolbe a călătorit în Elveţia transportând aproximativ 200 de documente sustrase din dosarele Ministerului de Externe de la Berlin. El a abordat iniţial Ambasada Britanică de la Berna. Încercând să evite "agenţi provocatori" sau agenţi germani, britanicii nu au dorit să aibă de a face cu Kolbe. Atunci, el l-a abordat pe Allen Dulles, şeful operaţiunilor secrete americane din Elveţia. Precaut, dar într-o măsură mai mică decât aliaţii britanici, americanii au lucrat cu Kolbe care, în urma unor călătorii ulterioare la Berna, le-a furnizat peste 1.500 de documente secrete germane. Kolbe a fost probabil unul dintre cei mai mari spioni din perioada războiului în favoarea Statelor Unite.[17]

În afară de o clasificare a surselor, mai putem realiza o diferenţiere a motivelor pentru care acestea furnizează informaţii. Sursele pot fi mânate de credinţe ideologice, etnice sau religioase mai puternice decât legăturile lor cu ţările ale căror cetăţeni sunt; este posibil ca acestea să fie deziluzionate de acţiunile sau ideologiile propriilor ţări; pot fi lacome; pot fi persoane cărora le lipseşte echilibrul interior şi doresc să aibă parte de aventură; doresc să se răzbune din cauza unui presupus tratament necorespunzător din partea guvernului; sau pot face obiectul unei acţiuni de şantaj. Importanţa relativă a acestor motive depinde de caracteristicile societăţilor implicate şi de tacticile serviciilor de informaţii adverse.

De exemplu, din trecutul acţiunilor de culegere de informaţii realizate de sovietici împotriva Statelor Unite şi Marii Britanii, începând din 1930, se desprinde ideea trecerii de la ideologie la lăcomie şi răzbunare, care constituie motive pentru unii americani şi britanici să-şi trădeze ţara. În 1930, sovieticii au aflat că atracţia pe care o exercita comunismul asupra unor studenţi şi asistenţi de la Universitatea Cambridge, unii provenind din familii de seamă, a făcut ca atmosfera ideologică să fie foarte favorabilă. Printre studenţii recrutaţi la vremea respectivă, care au devenit ulterior importanţi agenţi sovietici infiltraţi în guvernul britanic, se numără Guy Burgess, Donald Maclean şi Harold ("Kim") Philby.[18]

Pe de altă parte, americanii şi britanicii care au fost arestaţi pentru spionaj în favoarea Uniunii Sovietice la sfârşitul anilor 1970 şi 1980 par să fi fost motivaţi în special de lăcomie.[19] În alt caz, cel al lui Edward Lee Howard, fost ofiţer CIA care le-a oferit sovieticilor detalii operaţionale esenţiale privind activităţile agenţiei la Moscova, motivul a fost răzbunarea împotriva CIA, întrucât fusese concediat.[20]

În general, publicul supraestimează probabil utilizarea sexului în vederea obţinerii de secrete şi predominarea şantajului ca motiv pentru activităţi de spionaj, deşi posibilitatea de a recurge la şantaj îi poate permite unui ofiţer să-şi păstreze o sursă care a devenit spion din alte motive, iar ulterior intenţionează să renunţe. Chiar şi aşa, au ieşit la lumină unele cazuri care presupun folosirea seducţiei şi şantajului, în genul descrierilor din romanele de spionaj.

De exemplu, în perioada celui de-al Doilea Război Mondial, Betty Pack a avut o evoluţie similară cu a celebrei Mata Hari. Căsătorită cu un diplomat britanic, cetăţean american la origine, Pack a lucrat atât pentru

serviciile de informaţii britanice, cât şi pentru cele americane. Strategia ei s-a axat în special pe aventuri cu importanţi oficiali guvernamentali străini. Printre multele sale reuşite, aceasta a adunat informaţii diplomatice esenţiale de la ministerul polonez de Externe, înaintea războiului, a obţinut date importante referitoare la eforturile polonezilor de a sparge codurile criptate ale germanilor, a compromis definitiv lucrările Ambasadei Franceze (Vichy) de la Washington şi a obţinut coduri folosite de marina italiană şi de cea franceză.[21]

Totuşi, o metodă mai puternică decât seducţia este folosirea sexului pentru a atrage în cursă şi pentru a şantaja un oficial care are acces la materiale sau informaţii de importanţă deosebită. Un exemplu tipic de acest gen îl are în prim plan pe Maurice Dejean, ambasadorul francez la Moscova în anii 1950 şi 1960. Aflând despre caracterul imoral al ambasadorului căsătorit, KGB a angajat o femeie frumoasă (cetăţean sovietic forţat să coopereze) să-l seducă. După începerea aventurii, cuplul a fost surprins de întoarcerea "neaşteptată" a "soţului" acesteia. "Şocat", acesta a ameninţat să facă publică povestea şi să-l acţioneze în judecată pe ambasador. Dejean s-a confesat unui "prieten" rus – în realitate, ofiţerul superior KGB care îi înscenase povestea; "prietenul" s-a oferit să-l ajute pe acesta să păstreze secretul. Planul KGB viza folosirea acestei situaţii compromiţătoare în vederea şantajării lui Dejean, pentru a-l face să lucreze cu ei atunci când avea să se întoarcă în Franţa şi, în speranţa că acesta urma să primească un post mai înalt. Cu toate acestea, planul sovieticilor a fost năruit de defectarea unui scenarist rus, care participase la crearea intrigii.[22]

Probleme privind culegerea de informaţii din surse umane

Multe probleme privind culegerea de informaţii din surse umane sunt inerente naturii activităţii, în timp ce altele sunt specifice mai degrabă ţintei informaţiilor secrete. În ceea ce priveşte prima categorie, cea mai importantă este asigurarea calităţii controlului – având certitudinea că informaţiile furnizate de surse sunt corecte.

Din motive financiare, sursele pot fie să fabrice informaţii, fie să reorganizeze cu multă imaginaţie sau să înflorească materialele disponibile publicului, pentru a părea că provin din surse extrem de bine plasate (prin folosirea unui jargon al serviciilor de informaţii, crearea unui "*paper mill*" – documente prefabricate). Din trecutul serviciilor de informaţii se reflectă exemple ocazionale de creatori de asemenea documente prefabricate, care şi-au escrocat clienţii cu sume enorme de bani.

Acest tip de documente prefabricate au înflorit la sfârşitul anilor 1940 şi începutul anilor 1950, exploatând dificultatea serviciilor occidentale de informaţii de a opera în ţările comuniste din Europa de Est. Deseori acestea erau manipulate de emigranţi săraci din ţările respective, care au descoperit la scurt timp că îşi pot câştiga traiul prin vânzarea unor "informaţii" pe care susţineau că le primesc de la cunoştinţe aflate în poziţii de influenţă în noile guverne comuniste. Întrucât aceşti emigranţi aveau o

educație bună și cunoșteau dedesubturile politice, ei au fost capabili să înflorească și să interpreteze informațiile disponibile publicului pentru a produce rapoarte convingătoare de informații.[23]

O problemă mai gravă privind controlul calității decurge din posibilitatea ca un agent să fi fost "dublat" – ca acesta să lucreze în secret pentru presupusa țintă și ca informațiile pe care le furnizează presupușilor săi angajatori să fie menite să-i înșele. O asemenea dublare poate avea loc în momentul în care o sursă de informații este arestată și alege să coopereze cu cei care au capturat-o pentru a evita diverse pedepse.[24] Pe de altă parte, sursa putea fi un "agent dublu" (o presupusă sursă de informații care lucrează într-adevăr pentru țara pe care pretinde că o spionează) de la bun început, similar relatărilor de mai sus referitoare la voluntari.

Unele dintre cele mai interesante și remarcabile relatări din istoria serviciilor de informații privesc folosirea agenților dubli. De exemplu, în ceea ce s-a numit "sistem încrucișat", britanicii au reușit să preia controlul și apoi să manipuleze activitățile germanilor de culegere de informații din surse umane în Marea Britanie, în perioada celui de-al Doilea Război Mondial. Chiar de la începutul războiului, britanicii au controlat toate rapoartele cu informații transmise acasă de presupuși agenți germani în Marea Britanie. Printre alte reușite, aceste rapoarte au ajutat la inducerea în eroare a germanilor cu privire la locația și detaliile privind debarcarea din Normandia. Pe 9 iunie 1944, la trei zile după ziua Z, un mesaj trimis de o sursă controlată de britanici a avut o importanță vitală, ducând la blocarea unei divizii germane de tancuri în zona Calais (pentru a împiedica iminenta debarcare a "trupelor principale", care în realitate nu existau), și ajutând adevărata forță de invazie din Normandia să-și asigure avanposturile.[25]

Alte probleme au decurs din natura țintei. Cu cât este mai eficient și mai atotpătrunzător sistemul intern de securitate al unei țări vizate, cu atât apar mai multe dificultăți în vederea culegerii de informații din surse umane pe teritoriul țării respective. Un guvern care desfășoară un control minuțios asupra călătoriilor și comunicațiilor internaționale, precum și asupra altor mișcări, comunicații și activități economice ale cetățenilor săi, în general, poate îngreuna extrem de mult desfășurarea activităților neoficiale sub acoperire sau "ilegale" ale unor ofițeri de informații, care intenționează să călătorească în țara respectivă, să-și înceapă activitățile "secrete" și să opereze fără a fi depistați. Ofițerii care acționează oficial sub acoperire pot fi supuși unor acțiuni de supraveghere intensă, ceea ce le îngreunează întâlnirea cu diverși cetățeni ai țării țintă, fără a fi observați. Rezultatul este denumit în jargonul serviciilor de informații americane ca "țintă dificilă" sau "zonă interzisă", o țară în care activitățile de informații se pot desfășura în general numai sub acoperire oficială și, chiar și atunci, cu mare dificultate.

De asemenea, mai există și alte ținte care ridică probleme specifice. De exemplu, culegerea de informații legate de terorism este limitată de natura relativ restrânsă, secretă și extrem de omogenă a majorității grupărilor teroriste. (Observații similare se aplică culegerii de informații din surse umane împotriva crimei organizate.) Deoarece calitatea de membru al

acestor grupări se obține pe baza prieteniilor, a legăturilor de rudenie sau a activităților infracționale anterioare, devine din ce în ce mai dificilă introducerea unei surse de informații în rândul acestora (în jargonul serviciilor de informații, "penetrare"). În acelaşi context, loialitatea existentă într-o asemenea grupare (ca să nu mai vorbim despre disciplina pe care grupările o impun membrilor lor) îngreunează încercările de a convinge pe unul dintre membri să o trădeze.

Dificultățile nu se vor sfârşi niciodată, chiar dacă o sursă reuşeşte să se infiltreze într-o grupare teroristă. Pentru a rămâne membru permanent, sursa trebuie să asigure sprijin material pentru acțiuni teroriste sau să participe la acestea. Totuşi, majoritatea agențiilor de informații se simt obligate să stabilească anumite limite în privința acțiunilor pe care un ofițer sau sursă le poate desfăşura pentru a-şi păstra credibilitatea. În acelaşi timp, utilizarea informațiilor furnizate de sursă pentru a semnala sau contracara desfăşurarea unor acțiuni teroriste planificate poate indica teroriştilor că există un informator în mijlocul lor şi, în consecință, poate pune în pericol viața sursei. Astfel, este posibil ca agenția să poată analiza îndeaproape planurile interne ale grupărilor de acest gen, abia atunci când un membru a fost capturat.

Arta schimbului de informații

Metodele specifice pe care le foloseşte un ofițer de informații pentru a acționa şi comunica cu sursele sale, fără a fi detectat de serviciul de informații advers, sunt cunoscute sub denumirea de "artă a schimbului de informații". Cea mai gravă problemă cu care se confruntă un ofițer de informații este posibilitatea ca serviciul advers să-l supravegheze (adică, să-l monitorizeze şi să-l urmărească) pentru a-i controla activitățile şi pentru a identifica persoanele cu care acesta intră în contact. Prin urmare, misiunea ofițerului este aceea de a afla dacă se află sub supraveghere şi, dacă acest lucru se confirmă, de a scăpa de sub supraveghere atâta timp cât este necesar pentru a putea intra în contact cu sursele sale sau cu potențiale surse, fără a risca divulgarea identității acestora.[26]

O tehnică folosită pentru a scăpa de urmăritori, pe care CIA o predă ofițerilor, este ilustrată prin trucul utilizat de Edward Lee Howard – ofițer eliminat din serviciul CIA – pentru a scăpa de supravegherea FBI în 1985. Într-o seară, pe când se întorcea acasă, iar soția sa se afla la volan, suspectând că este urmărit de FBI, Howard i-a cerut soției să vireze brusc într-o intersecție întunecată; imediat după viraj, acesta a deschis portiera din dreapta şi s-a aruncat afară. În acelaşi timp, soția lui Howard a umflat o păpuşă în locul lui, făcând să pară de la distanță că Howard încă se mai afla în maşină. Ea a mers acasă, a intrat în garaj şi a închis uşa garajului, fără a oferi nici un indiciu echipei de urmărire că Howard scăpase de ei şi că era liber să se mişte, fără a fi urmărit.[27]

În acelaşi fel, până să ajungă într-un loc de întâlnire, un ofițer poate parcurge drumul în câteva ore, creându-şi un adevărat circuit şi folosind mijloace de transport diferite. Dacă acesta observă că persoana care stă lângă

el în metrou, a stat lângă el şi în autobuz, el poate concluziona în mod logic că este urmărit. Echipa de supraveghere poate să nu fie depistată dacă foloseşte un anumit sistem astfel încât un ofiţer să nu fie urmărit de acelaşi individ pe parcursul unei călătorii. Jocul supravegherii şi al depistării acesteia poate fi complicat aproape la nesfârşit.[28]

Arta schimbului de informaţii include, de asemenea, tehnici de comunicare cu o sursă, fără a fi necesară o întâlnire. De exemplu, un ofiţer poate înmâna discret unei surse un pachet sau un document, în trecere, pe stradă ("predare fulger"). Dacă acest lucru este realizat corect, manevra poate nici să nu fie observată de echipa de supraveghere. Ofiţerul îşi poate amplasa servieta pe jos, lângă scaunul său, în timp ce serveşte o băutură într-o cafenea; sursa se aşează la masa vecină şi îşi pune pe jos servieta, aproape identică cu cea a ofiţerului, lângă cealaltă. Când sursa pleacă, ia servieta ofiţerului în loc să o ia pe a sa. Din nou, cu excepţia cazului în care echipa de supraveghere a observat manevrarea servietelor, este posibil ca schimbul nici să nu fie observat.

În acelaşi mod, un ofiţer poate lăsa un bilet într-o locaţie stabilită anterior, cum ar fi în scorbura unui copac dintr-un parc; câteva ore mai târziu, sursa îl recuperează ("cutie poştală impersonală").[29] Dacă ofiţerul plasează biletul fără a fi observat, cel care se află pe urmele sale cu scopul de a afla identitatea surselor, va continua pur şi simplu să-l urmărească, fără să realizeze că întâlnirea a avut deja loc. Robert P. Hanssen, specialist în contra-informaţii al FBI, condamnat recent pentru spionaj în favoarea Uniunii Sovietice şi apoi a Federaţiei Ruse pentru o perioadă de peste 15 ani, a comunicat în majoritatea cazurilor prin metoda "cutiei poştale impersonale"; evident, cunoscând foarte bine procedurile FBI, acesta a considerat metoda menţionată ca fiind cea mai sigură.[30]

O altă măsură de precauţie este evitarea stabilirii întâlnirilor cu o sursă într-o ţară împotriva căreia aceasta spionează. Este probabil mult mai sigur ca întâlnirea să aibă loc într-o ţară terţă, unde echipele de supraveghere pot fi mai puţin vigilente sau chiar inexistente. De exemplu, Uniunea Sovietică a preferat deseori să stabilească întâlniri cu surse americane, cum ar fi John Walker (care le-a furnizat sovieticilor cantităţi semnificative de informaţii clasificate privind comunicaţiile şi operaţiunile maritime) în Austria, o ţară care, deşi cu un stil democratic occidental, şi-a declarat oficial neutralitatea în timpul Războiul Rece.

> *Cazul Walker a dezvăluit atenţia pe care sovieticii o acordă unui agent important. Majoritatea întâlnirilor cu sovieticii au avut loc la Viena, Austria… În timpul acestor întâlniri, Walker şi persoana lui de contact de la KGB obişnuiau să se plimbe pe străzi [,] … [fără a utiliza vreodată] o casă conspirativă în care să se întâlnească, întrucât persoana de contact tocmai venise de la Moscova iar* rezidentura *din Viena (organizaţia, grup de ofiţeri KGB care lucrau în afara ambasadei sovietice) nu cunoştea informaţii cu privire la această operaţiune.*[31]

În alte cazuri, serviciile de informaţii care operează împotriva Statelor Unite au preferat să-şi întâlnească sursele în Canada sau Mexic. Alegerile sunt justificate, având în vedere uşurinţa cu care americanii se pot deplasa în ţările respective şi numărul mare de americani care fac acest lucru. De exemplu, lingvistul şi analistul CIA, Larry Wu-tai Chin, spion pentru o lungă perioadă de timp în favoarea Republicii Populare Chineze, a efectuat deplasări frecvente la Toronto pentru a primi informaţii de la sursa lui şi pentru a-i înmâna acesteia un film nedevelopat.[32]

Alte metode clasice privind comunicarea dintre ofiţerii de informaţii şi sursele lor, fără a fi necesară o întâlnire fizică, presupun "scrieri secrete" şi "micro-puncte". Aceste tehnici sunt utile în cazurile în care ofiţerul şi sursa au un motiv aparent inocent de a comunica unul cu celălalt, dar suspectează că există posibilitatea ca scrisorile lor să fie deschise şi citite de partea adversă. Pentru a folosi scrierea secretă, ofiţerul sau sursa va scrie mai întâi o scrisoare aparent inofensivă. Folosind o hârtie de indigo, tratată special, el va scrie apoi un mesaj secret pe deasupra scrisorii originale. Mesajul este invizibil ochiului liber şi devine lizibil numai când hârtia este tratată cu un agent chimic special, cunoscut numai de serviciul de informaţii pentru care lucrează ofiţerul şi sursa. Micro-punctele reprezintă o metodă secundară de comunicare; în această situaţie, fotografiile sunt micşorate la dimensiuni microscopice şi ascunse într-un anumit loc pe hârtie, poate chiar sub o ştampilă sau deasupra semnelor de punctuaţie, în cazul literelor dactilografiate.

Defectorii

Până acum, discuţiile s-au axat numai pe sursele de informaţii care rămân în funcţie – adică raportează informaţii în timp ce îşi păstrează poziţia oficială ce le permite acces la acestea. Aceasta este în mod evident cea mai bună situaţie în cazul culegerii de informaţii, din moment ce presupune păstrarea accesului la informaţii, precum şi posibilitatea de a "însărcina" sursa cu obţinerea unor documente sau fragmente de informaţii specifice, necesare sau utile. Acest lucru presupune ca orice comunicare dintre o sursă şi agent să rămână secretă, iar sursa riscă să fie prinsă.

Într-o zonă greu accesibilă, aceste dificultăţi se amplifică. În consecinţă, culegerea de informaţii din surse umane împotriva unor asemenea ţări depinde adesea foarte mult de defectori. Din punctul de vedere al serviciilor de informaţii, acestea constituie surse care nu rămân pe loc, ci mai degrabă fug din ţările de proveniență, de obicei ilegal, şi primesc azil. În perioada ulterioară celui de-al Doilea Război Mondial, culegerea de informaţii din surse umane din Occident împotriva Uniunii Sovietice a depins în mare măsură de astfel de indivizi. De exemplu, la începutul anilor 1950, serviciile occidentale de informaţii nu au avut mare succes în recrutarea de ofiţeri sovietici de informaţii. Cu toate acestea, în 1954, într-un interval de patru luni, cinci ofiţeri au defectat în Occident. Aceste defectări au rezultat într-o cantitate enormă de informaţii privind operaţiunile

serviciilor sovietice din primii zece ani după încheierea celui de-al Doilea Război Mondial. În urma defectărilor, s-au aflat importante informații secrete privind practicile KGB şi arta desfăşurării operațiunilor, eforturile organizației de a decripta codurile folosite de alte guverne, penetrările agenților KGB în guvernele occidentale şi implicarea acestora în asasinate.[33] Similar, defectarea lui Hussein al-Kamal, ginerele dictatorului irakian Saddam Hussein, în august 1995, a oferit informații valoroase referitoare la programul secret al Irakului privind dezvoltarea de arme biologice care nu fuseseră descoperite în timpul inspecției realizate de Comisia Națiunile Unite (UNSCOM) de-a lungul unei perioade de patru ani.[34]

În ciuda importanței lor, defectorii pun aceleaşi probleme ca voluntarii. Este greu să fii sigur că aceştia sunt într-adevăr defectori, şi nu cetățeni loiali trimişi de guvernul țării lor pentru a dezinforma rivalii. Se impune un oarecare scepticism în relația cu aceştia, cel puțin la început. Informațiile contradictorii furnizate de unii defectori sovietici de seamă în Statele Unite – în special, cu privire la prezența sau absența unei cârtițe sovietice plasate într-o poziție înaltă în guvernul american – nu au fost nici până în prezent pe deplin deslușite; acestea au pus în dificultate serviciul american de informații de-a lungul unui sfert de secol.[35]

CULEGEREA DE INFORMAȚII DIN SURSE TEHNICE

Culegerea de informații din surse tehnice (sau techint, în jargonul serviciilor americane) se referă la un set de tehnici care folosesc mai degrabă tehnologia avansată, decât agenți umani, în vederea culegerii de informații. Limitate în ultimă instanță numai de ingeniozitatea umană şi de legile fizicii, aceste tehnici presupun fotografierea de la distanță mare şi interceptarea unor unde electromagnetice, deşi se exploatează, de asemenea, şi alte mecanisme (de exemplu, semnale acustice).

Informații rezultate din fotografii şi imagistică

Informațiile rezultate din fotografii şi imagistică (photint sau imint), aşa cum relevă denumirea, se referă la fotografierea în vederea culegerii de informații. Mai exact, se realizează fotografii de la distanță pentru a obține imagini ale unor locații sau obiecte, la care nu este posibil accesul direct. Această idee a fost pusă în practică sub forma unei supravegheri aeriene, apărută aproape în acelaşi timp cu inventarea avionului.[36]

La începutul Primului Război Mondial, în august 1914, Forțele Aeriene Regale Britanice au condus supravegherea aeriană asupra trupelor germane care înaintau prin Belgia.[37] Odată cu încheierea primei perioade a mişcării, când germanii şi armatele aliate s-au trezit față în față de-a lungul unui front ce se întindea din Elveția până în Marea Nordului, supravegherea aeriană a fost considerată un substitut pentru acțiunile de patrulare ale cavaleriei, care nu mai puteau parcurge zona aflată de-a lungul şi din spatele

armatei inamice. Aşa cum a scris Generalul de Brigadă William Mitchell, apostolul american al forței aeriene din perioada dintre cele două războaie, "Un zbor deasupra frontului mi-a oferit o imagine mult mai clară asupra modului în care erau dispuse armatele, decât mi-ar fi oferit o patrulare la sol"[38]. De aici şi până la amplasarea de camere de luat vederi pe aceste avioane şi dezvoltarea unei capacități aeriene de foto-recunoaştere, nu a fost decât un pas.

Odată cu dezvoltarea ulterioară a aviației şi fotografiei, foto-recunoaşterea aeriană a devenit o sursă importantă de informații secrete în timpul celui de-al Doilea Război Mondial. Această metodă a fost utilizată nu numai pentru a depista dispunerea şi mişcarea forțelor inamice, ci şi pentru a urmări progresele tehnologice. Prin urmare, britanicii au folosit foto-recunoaşterea aeriană, precum şi alte surse de informații, pentru a spiona descoperirile tehnice ale germanilor, cum ar fi sistemele radiogoniometrice pe care germanii le-au inventat pentru
a-şi ghida bombardierele către ținte din Anglia, noile radare aeriene de apărare şi rachetele V-1 şi V-2.

Până acum, exemplele oferite din domeniul foto-recunoaşterii au fost din perioada războiului; acest lucru nu este întâmplător. În perioada războiului interesele armate în vederea realizării unor asemenea activități au fost mai mari, iar obstacolele politice prea puține. Nu numai că este mai important să cunoaştem evenimentele care se petrec în țara inamică pe timp de război, ci şi faptul că metodele alternative pentru a afla aceste lucruri sunt extrem de puține. Nu ne putem baza numai pe rapoarte primite de la jurnalişti, călători, diplomați sau ataşați; în general, relatările din presă sunt îndeaproape controlate, granițele sunt închise, iar călătoriile în interiorul țării țintă sunt restricționate, atât pentru proprii cetățeni ai țării, cât şi pentru cetățeni ai altor țări neutre. În acelaşi timp, legea internațională care interzice survolarea unei alte țări fără consimțământul acesteia nu mai reprezintă un obstacol politic.

Chiar şi aşa, dificultățile cu care s-au confruntat Statele Unite în încercarea de a desfăşura activități de culegere de informații din surse umane împotriva Uniunii Sovietice de-a lungul anilor imediat următori încheierii celui de-al Doilea Război Mondial, le-au făcut să ia în considerare posibilitatea utilizării activității de foto-recunoaştere pe timp de pace. Acest interes a fost consolidat atunci când, în 1950, exista temerea ca nu cumva invadarea Coreei de Sud de către Coreea de Nord să constituie un imbold pentru o invazie sovietică în Europa de Vest. Din cauza insuficienței surselor umane de informații, Statele Unite s-au temut că pregătirile sovieticilor pentru o asemenea invazie ar putea nici să nu fie detectate. În plus, nu prea existau informații privind "ordinul de atac" al sovieticilor (dimensiunea şi structura forțelor armate), lucru care îngreuna extrem de mult eforturile guvernului american de a evalua necesarul propriu de cheltuieli din domeniul militar.

Un exemplu de lipsă de date concrete privind forțele sovietice l-a constituit presupusul "decalaj al bombardierului" la jumătatea anilor 1950.

Statele Unite deţineau extrem de puţine informaţii referitoare la planurile sau capacităţile sovietice pentru construirea unui bombardier strategic sau "înarmat" (un avion capabil să transporte o armă nucleară la distanţe mari între continente). Cu toate acestea, la ceremonia de sărbătorire a Zilei Forţelor Aeriene Sovietice, în iulie 1955, imediat înaintea Summit-ului de la Geneva a celor "Patru mari puteri" (Statele Unite, Uniunea Sovietică, Franţa şi Marea Britanie), un ataşat al forţelor aeriene americane a văzut survolând 28 de bombardiere de mari dimensiuni, un model relativ nou. Se pare că sovieticii demaraseră un program în vederea construirii unor bombardiere strategice care, date fiind planurile de apărare ale SUA, urmau să deschidă un abis considerabil – denumit "decalajul bombardierului" – între capacităţile americanilor şi ale sovieticilor în acest domeniu. Totuşi, ataşatul fusese păcălit de un simplu vicleşug: el nu văzuse 28 de bombardiere noi, ci un număr mai mic care au survolat zona de mai multe ori.[40] Cu toate acestea, în absenţa unor informaţii concrete, raportul ataşatului a devenit punctul de pornire în vederea solicitărilor de creştere a bugetului american pentru domeniul apărării.

S-au făcut mai multe încercări pentru a se depăşi această lipsă de informaţii privind armata sovietică. Unul dintre proiecte, denumit "Moby Dick", presupunea lansarea unor baloane în Europa de Vest, echipate cu camere de luat vederi, îndreptate spre pământ. Ideea era ca aceste baloane să ajungă apoi în Uniunea Sovietică, purtate de vânturile dinspre vest, până ajungeau în Japonia sau în Oceanul Pacific. În acel moment, camerele urmau să fie desprinse printr-un semnal radio şi recuperate. În realitate, multe dintre baloanele respective au aterizat în Uniunea Sovietică, permiţându-le sovieticilor să analizeze tehnologia camerelor. În orice caz, din cauza mişcării necontrolate a baloanelor deasupra Uniunii Sovietice, fotografiile developate de pe filmele recuperate au dezvăluit probabil informaţii nesemnificative.[41]

Pe 21 iulie 1955, la Summit-ul celor "Patru mari puteri", Preşedintele Dwight D. Eisenhower a propus planul "Spaţiilor Aeriene Deschise" care viza supravegherea reciprocă a Statelor Unite şi URSS. Conform planului, urma ca cele două ţări "să-şi ofere reciproc un plan complet al obiectivelor militare … dintr-un capăt al ţării până în celălalt," fiecare urmând să aibă dreptul de a desfăşura activităţi de supraveghere aeriană asupra teritoriului celeilalte aşa cum considera de cuviinţă.[42] Eisenhower era de părere că acest plan avea să împiedice orice încercare de a lansa un atac neaşteptat; în opinia sa, un potenţial atacator nu putea spera să surprindă cu un atac dacă era supus unei supravegheri aeriene permanente. Supravegherea avea, de asemenea, să faciliteze semnarea unor acorduri ulterioare de dezarmare, deoarece cu ajutorul acesteia se putea stabili dacă cealaltă parte îşi respectă obligaţiile.

Cu toate acestea, Eisenhower nu a dorit să-şi condiţioneze planurile în vederea desfăşurării unor activităţi mai eficiente de culegere de informaţii despre sovietici. Opt luni mai târziu, pe 24 noiembrie 1954, acesta a aprobat în secret construirea unui nou avion care să desfăşoare misiuni de

recunoaştere, U-2, care putea să zboare la înălţimea la care zburau avioanele de luptă ale sovieticilor şi rachetelor sol-aer (SAM). În plus, s-a anticipat că foto-recunoaşterea din sateliţi era o idee fezabilă.[43] În orice caz, premierul sovietic Nikita Hruşciov, a respins propunerea privind "Spaţiile aeriene deschise", caracterizând-o drept o încercare de legalizare a spionajului. Pe 21 iunie 1956, Eisenhower a aprobat în secret primul zbor al avionului U-2 deasupra teritoriului sovietic.[44]

De-a lungul următorilor patru ani, zborurile U-2, efectuate atât deasupra teritoriului sovietic, cât şi de-a lungul graniţelor sale, au oferit o multitudine de informaţii, au furnizat pentru prima dată Statelor Unite o imagine de ansamblu asupra unor importante facilităţi şi baze militare sovietice de testare. Sovieticii au protestat pe căi diplomatice împotriva survolărilor, însă, în primă fază, nu au putut să facă nimic în acest sens. Totuşi, a fost doar o problemă de timp până ce sovieticii au elaborat o serie de mijloace capabile să atace avioanele U-2. Pe 1 mai 1960, aceştia au reuşit să doboare unul dintre avioane, capturând pilotul, Francis Gary Powers.

Cu toate acestea, chiar înaintea incidentului în care a fost implicat avionul U-2, Statele Unite demaraseră construcţia unui satelit cu capacităţi de foto-recunoaştere.[45] Cu toate că în timpul stadiului de elaborare[46] s-a discutat în mod deschis despre construirea acestei staţii, existenţa sa a fost, pentru început, considerată ca fiind strict secretă.[47] Totul a rămas secret până în 1978, când preşedintele Jimmy Carter, dorind să justifice cel de-al doilea tratat SALT (Tratatul privind reducerea armelor strategice) în faţa poporului american, a confirmat public că Statele Unite deţineau o astfel de resursă; existenţa sa fusese un secret timp de mai mulţi ani. Odată cu încheierea Războiului Rece, existenţa şi identitatea Biroului Naţional de Recunoaştere (NRO) – agenţie cu atribuţii în "cercetarea şi dezvoltarea, achiziţionarea şi operarea sistemelor de culegere de date din spaţiul cosmic şi din spaţiul aerian" menită "să respecte nevoile de informaţii ale guvernului SUA" – au fost declasificate.[48]

Esenţa activităţilor de foto-recunoaştere o reprezintă calitatea şi puterea echipamentelor optice utilizate pentru captarea şi concentrarea luminii reflectate de obiecte aflate pe pământ. Alegerea altitudinii la care se deplasează satelitul presupune un compromis între calitatea imaginii (alte aspecte fiind egale, cu cât se deplasează mai jos pe orbită, cu atât va fi mai bună calitatea) şi intervalul de timp în care satelitul se poate ridica (dacă satelitul traversează sferele mai înalte din atmosfera pământului, rezistenţa pe care o manifestă atmosfera îl va încetini şi va face ca greutatea lui să-l atragă spre pământ). Alţi factori care determină deplasarea pe orbită se referă la cerinţe privind optimizarea capacităţii de fotografiere a anumitor părţi ale suprafeţei pământului şi amplasarea unui satelit în funcţie de poziţia soarelui pentru ca fotografiile să fie făcute în condiţii optime de lumină. O dificultate aparte întâlnită în fotografiile făcute în spaţiu este aceea că lumina trebuie să penetreze întreaga atmosferă, care are tendinţa de a o difuza, ducând astfel la estomparea imaginii. Pe de altă parte, camerele folosite pentru captarea imaginilor din spaţiu, spre deosebire de cele amplasate pe avioane, nu sunt

expuse la vibrațiile produse de motorul unui avion cu reacție sau la turbulențele atmosferice.[49]

La început, toți sateliții folosiți pentru acțiuni de foto-recunoaştere foloseau camere de filmat puternice care, la o comandă efectuată de la sol, evacuau filmul într-o capsulă; capsula era recuperată în timp ce cobora din spațiu, iar filmul era developat şi analizat. Din anumite motive – cum ar fi deplasarea îndelungată într-o anumită direcție sau identificarea şi localizarea obiectivelor militare fixe – timpul scurs între momentul fotografierii şi developarea şi analizarea fotografiilor nu a constituit o problemă. Cu toate acestea, a apărut o dificultate legată de sistemul de recuperare a filmelor, mai exact de legătura cu țintele mobile sau evenimentele care se desfăşurau rapid. De exemplu, o întârziere de câteva zile ar putea duce la eşecul unui atac prin surprindere.

Pentru a accelera procesul, filmul poate fi înlocuit cu un dispozitiv de semiconductori sensibili la lumină cunoscut sub numele de circuit cu cuplaj de sarcină (CCD). Odată ce lumina atinge unul dintre aceşti semiconductori, se produce un semnal electric proporțional cu intensitatea luminii. Măsurând magnitudinea acestor semnale asupra unor elemente individuale ale CCD şi notând cu exactitate unde anume se află fiecare element în grilă, un procesor poate reconstitui din aceste informații o imagine fie pe film, fie pe terminalul unui computer. Întrucât există o întârziere infimă din momentul transmiterii electronice a datelor din spațiu către o stație aflată la sol, imaginea unei ținte poate fi reprodusă pe pământ aproape "în timp real" – adică, cu o întârziere nesemnificativă.[50]

În ciuda acestor îmbunătățiri, orice capacitate de foto-recunoaştere încă mai depinde de lumina soarelui şi de absența umbrei produsă de un nor. Pentru a depăşi aceste limitări, prin folosirea radiolocatoarelor sau undelor prin infraroşu (emise de obiecte calde sau fierbinți), se pot folosi alte tipuri de imagini. De exemplu, în loc să se bazeze pe lumina soarelui, reflectată în mod natural de un obiect de pe pământ pentru a produce o imagine, un sistem de recunoaştere cu radiolocator transmite propriile unde radio către zona țintă de jos, recuperează undele reflectate de diverse obiecte şi, printr-un proces complex, converteşte datele respective într-o imagine.[51] Prin "luminarea" țintelor, independent de soare, şi folosirea lungimilor de undă care pot penetra norii, ceața sau precipitațiile, sistemele de recunoaştere cu radiolocatoare pot asigura o capacitate de capturare a imaginilor, în orice condiții meteorologice, pentru o perioadă de 24 de ore.

Similar, o altă componentă a spectrului electromagnetic, undele infraroşii, poate fi utilizată pentru detectarea obiectelor care sunt mai calde (sau mai reci) decât altele din jurul lor. De exemplu, pe timpul zilei, formarea imaginilor prin infraroşu permite desluşirea frunzişului (care are o "semnătură" de căldură) de orice camuflaj (care are o alta). Pe timpul nopții, întrucât obiectele încălzite pe timpul zilei au ritmuri diferite de răcire, un sistem cu infraroşu poate permite unui analist să detecteze mai multe tipuri de obiecte şi ținte. De exemplu, la apus, obiectele metalice, cum ar fi tancurile, se răcesc mult mai lent decât terenul sau vegetația din jur; această

diferență poate fi surprinsă printr-un sistem de captare a imaginilor prin infraroşu, facilitând localizarea tancurilor respective la asfințit.[52]

Oricât de impresionante şi utile pot fi aceste capacități de recunoaştere prin imagini, ele prezintă totuşi un neajuns – calitatea imaginilor pe care le produc. În general, rezoluția (în general vorbind, dimensiunea celui mai mic obiect care poate fi detectat) fotografiilor realizate la lumină naturală este mai bună decât a fotografiilor realizate prin intermediul undelor radiolocatoare sau a altora din spectrul electromagnetic. Pentru anumite scopuri, cum ar fi mişcarea în masă a trupelor, imaginile cu rezoluție scăzută asupra unei zone întinse pot fi suficiente. Cu toate acestea, pentru alte cerințe, cum ar fi constatarea caracteristicilor tehnice ale unui sistem special de arme, se impune o mai mare precizie. Un factor determinant în implementarea eficientă a unor asemenea sisteme diferite de surprindere a imaginilor este cunoaşterea nivelului rezoluției necesar pentru a răspunde întrebărilor pe care le-ar putea avea guvernul referitor la potențialii săi adversari sau rivali pe câmpul de luptă.

A trecut mult timp de când activitățile de foto-recunoaştere din spațiu au început să constituie apanajul exclusiv al serviciilor de informații americane şi sovietice. Şi alte țări şi-au lansat proprii sateliți pentru a efectua fotografii în scopul obținerii de informații şi, odată cu dezvoltarea tehnologiilor relevante, din ce în ce mai multe țări pot face acest lucru, dacă doresc şi îşi permit să cheltuiască resursele necesare. Printre țările care şi-au lansat proprii sateliți sau intenționează să facă acest lucru se numără China, Franța şi Japonia.[53]

O măsură în acest sens a reprezentat dezvoltarea capacităților de foto-recunoaştere în scopuri comerciale. În 1986, o agenție guvernamentală din Franța a lansat un satelit de captare a imaginilor în scop de recunoaştere (Satellite pour l'Observation de la Terre [SPOT], sau "satelitul pentru observarea pământului") care a oferit spre vânzare fotografii alb-negru la o rezoluție pe zece metri. În 1999, Ikonos, o companie din SUA, a intrat pe piață cu o fotografie cu o rezoluție pe un metru; planurile companiei au fost acelea de a oferi fotografii cu o precizie chiar mai mare (o rezoluție pe jumătate de metru) începând din 2004, şi a primit deja permisiunea guvernului SUA de a realiza aceste lucruri.[54] Alte servicii comerciale de recunoaştere sunt oferite sau planificate de companii sau agenții guvernamentale din Rusia, Africa de Sud, Canada, India, Australia, Israel, China şi Brazilia.[55]

Culegerea informațiilor din semnale

Culegerea informațiilor din semnale (sau sigint) reprezintă procesul de extragere de informații din unde electromagnetice interceptate, denumite în general semnale. În funcție de tipul de unde electromagnetice interceptate, acest tip de culegere de informații se poate împărți în următoarele categorii:

- Obținerea de informații prin interceptarea comunicațiilor străine (mesaje radio) de către altcineva decât destinatarul țintă, sunt cunoscute ca informații obținute din comunicații sau COMINT.
- Interceptarea, procesarea şi analizarea telemetriei străine (semnale radio care transmit inginerilor informații de la senzori aflați la bordul unui vehicul de testare, cu privire la caracteristicile de zbor sau la performanțe), sunt cunoscute ca informații obținute din telemetrie sau TELINT.
- Interceptarea, procesarea şi analizarea radiațiilor electromagnetice care nu sunt emise de un sistem de comunicații, ci provin de la un echipament militar (cum ar fi un radar) în timpul funcționării, sunt cunoscute ca informații obținute din surse electronice sau ELINT.
- În principiu, orice undă electromagnetică, emisă fie ca o parte necesară sau ca un derivat al funcționării unui echipament electric, face subiectul interceptării unui receptor corect amplasat şi reglat şi suficient de sensibil.[57]

Informații obținute din comunicații (COMINT)

Din această varietate de informații obținute din semnale, cea mai veche este COMINT, practic contemporană cu utilizarea undelor radio pentru comunicațiile militare şi diplomatice.[58] Spre sfârşitul celui de-al Doilea Război Mondial, COMINT (combinată cu analiza metodelor de criptare – prin spargerea codurilor şi cifrurilor folosite la transmiterea mesajelor importante)[59] a fost, conform informațiilor disponibile, mai importantă decât orice altă sursă de informații pentru marile puteri, atât pe timp de pace, cât şi pe timp de război.[60]

Una dintre primele utilizări ale COMINT, documentată public, a avut loc în timpul Primului Război Mondial, atunci când marina britanică a depus eforturi pentru a afla la timp dacă Germania intenționa să se aventureze în Marea Nordului. În plus, la începutul războiului, britanicii au deteriorat cablurile de telegraf submarine ale germanilor care legau Germania de America, Africa şi Spania. În consecință, "telegramele" diplomatice dintre Germania şi zonele respective trebuia să fie trimise prin radio, riscând să fie interceptate de stațiile britanice de monitorizare.[61]

În ciuda succeselor timpurii, Al Doilea Război Mondial a fost evenimentul care a marcat perioada de înflorire a activității de culegere a informațiilor din comunicații de către britanici, precum şi de americani. Sub denumirile de "Ultra" şi "Magic", comunicațiile germanilor şi japonezilor au fost interceptate şi decodate, iar cantități enorme de informații exacte au fost puse cu operativitate la dispoziția liderilor politici şi militari din Marea Britanie şi America. În timp ce evaluarea adevăratelor proporții ale impactului său asupra desfăşurării războiului rămâne în continuare o misiune

istorică dificilă, cu siguranță COMINT a jucat un rol inestimabil în înfrângerea Aliaților de către puterile Axei.[62]

Unul dintre cele mai concrete cazuri în care a fost esențială contribuția COMINT a fost victoria Marinei SUA asupra japonezilor în bătălia de la Midway. Japonia spera să profite de succesul său remarcabil de la Pearl Harbor, din decembrie 1941, punând stăpânire asupra insulei Midway, amplasată strategic, şi în acest proces, distrugând ce a mai rămas din forțele navale americane în Oceanul Pacific. Dacă ar fi reuşit planul japonezilor, Hawaii ar fi fost vulnerabilă în fața invaziei, iar Statele Unite s-ar fi văzut nevoite să cadă la o înțelegere de pace în condițiile impuse de Tokyo. Pentru japonezi era esențială o victorie rapidă în Pacific din moment ce lupta într-un război prelungit cu Statele Unite, o forță cu mai multă populație şi putere, ar fi dus la un eventual dezastru.

Fără ştirea japonezilor, criptologii marinei SUA din Hawaii au interceptat şi decodat comunicațiile criptate ale marinei japoneze. Prin urmare, forțele americane au aflat dinainte despre planul de atac al Japoniei asupra Midway.[63] Pe 4 iunie 1942, înarmat cu aceste informații, amiralul Chester Nimitz a organizat o ambuscadă asupra flotei navale japoneze, în nordul insulei, distrugând patru portavioane inamice şi eliminând aproape în totalitate capacitatea Japoniei de a mai desfăşura operațiuni de o asemenea amploare în Pacific. Bătălia de la Midway a reprezentat o înfrângere decisivă a japonezilor şi un moment de răscruce al războiului; aceasta a pus capăt oricăror speranțe ale japonezilor de a câştiga rapid războiul, asta dacă mai sperau la acest lucru.[64]

Deşi ne-am aştepta ca cele mai importante mesaje radio ale unei țări să fie criptate pentru a li se proteja confidențialitatea, unele sfere ale informațiilor obținute prin comunicații sunt independente de analiza criptică. Din cauza cheltuielilor şi dificultăților, este posibil ca un anumit trafic pe unde radio să nu fie criptat; de exemplu, comunicațiile tactice prin voce, cum ar fi între piloții avioanelor şi stațiile de control de la sol, sunt deseori emise "în eter". În alte situații, traficul de mesaje nu este codificat deoarece se crede că, în mod justificat sau nu, un adversar nu dorește sau nu poate să intercepteze sau (din cauza volumelor mari de informații) să le proceseze. De exemplu, traficul comercial nu este codificat de obicei, deşi o parte din acesta ar putea constitui subiect de interes pentru un potențial adversar. În sfârşit, nu trebuie să subestimăm importanța simplei inerții: de exemplu, Statele Unite au răspuns tardiv după ce s-a descoperit că traficul comunicațiilor telefonice, efectuate la distanțe mari, transmis prin piloni cu microunde, era interceptat de alte țări din locații diplomatice amplasate pe teritoriul țării lor.[65]

În plus, printr-o tehnică cunoscută ca "analiza traficului" se pot obține informații utile din fluctuații ale volumului şi alte caracteristici externe ale comunicațiilor radio, chiar şi atunci când conținutul mesajelor nu poate fi înțeles. De exemplu, dacă între sediul general al unei armate şi posturile de comandă din subordinea sa se efectuează un schimb neobişnuit de mare de mesaje, un analist poate concluziona că urmează să aibă loc o

operaţiune importantă.[66] Similar, prin mijloace de "depistare a direcţiei" sau prin "DF" – tehnică folosită pentru stabilirea zonei geografice din care provine un semnal radio – se poate localiza nava, avionul sau postul de comandă care îl transmite.

De exemplu, în al doilea Război Mondial submarinele germane (U-boats) care acţionau în largul mării îşi foloseau staţiile radio pentru a comunica între ele şi cu înaltul comandament al forţelor navale aflate pe uscat. Utilizarea de către flota germană a tacticii "haitei de lupi" împotriva convoaielor Aliate impunea un volum important de transmisiuni între submarinele germane şi comandamentul lor pentru a coordona şi a concentra atacurile. Totuşi, acest lucru a făcut submarinele vulnerabile la acţiunile de radio - goniometrie realizate de posturile britanice şi americane de interceptare radio şi de navele de război care escortau convoaiele. Deşi nu la fel de valoroase ca decriptarea efectivă a comunicaţiilor navale germane, operaţiunile de radio - goniometrie ale Aliaţilor au reprezentat un instrument important de culegere de informaţii în Bătălia Atlanticului. În combinaţie cu spargerea de coduri, au făcut posibil ca multe dintre convoaiele Aliaţilor să evite haitele de lupi germane în totalitate şi, în timp, au contribuit la eforturile americane şi britanice de a urmări şi scufunda submarinele germane.[67]

Deşi cea mai mare parte a surselor tehnice secrete (comint) presupune interceptarea mesajelor radio, pot fi interceptate şi mesajele care sunt transmise prin telegraf. Acest lucru necesită acces fizic la telegraf şi, astfel, are o aplicabilitate generală mai mică decât acele surse tehnice secrete, care implică trafic radio, deşi, în anumite cazuri, poate fi important. De exemplu, pot fi uşor menţinute dispozitive de interceptare pe liniile telefonice de la ambasada sau consulatul unui stat inamic din propria ţară.

Din când în când, este posibilă obţinerea accesului clandestin, chiar şi în afara graniţelor propriei ţări, la cablurile de telefon sau telegraf pe care le foloseşte un inamic. De exemplu, în oraşele divizate Viena şi Berlin la începutul şi mijlocul anilor 1950, serviciile de informaţii britanice şi americane au reuşit să pună dispozitive de interceptare pe cablurile folosite de autorităţile militare sovietice. În Berlin, acest lucru a implicat crearea unui tunel secret complicat dintr-un punct aflat în zona americană a oraşului pe sub linia de demarcaţie a acestei zone, pentru a intercepta cabluri care se aflau în întregime în interiorul zonei sovietice.[68]

O tehnică asemănătoare este montarea dispozitivelor de interceptare pe cablurile submarine utilizate de un stat inamic. De exemplu, în anii 1970, scafandrii dintr-un submarin american au fixat un dispozitiv de interceptare, în adâncul Mării Ohotsk, pe un cablu submarin sovietic ce lega baza navală sovietică de la Petropavlovsk din Peninsula Kamcatka cu Vladivostok şi Moscova. Scafandrii au ataşat un dispozitiv care înregistra convorbirile; înregistrările erau ridicate în timpul vizitelor periodice la locul respectiv.[69]

De asemenea, prin mijloace clandestine, este posibilă obţinerea accesului chiar la echipamentul folosit pentru trimiterea sau primirea de comunicaţii codificate. De exemplu, un fost ofiţer de informaţii britanic

povesteşte cum a reuşit serviciul de informaţii la care a lucrat să compromită comunicaţiile diplomatice egiptene prin plasarea unui dispozitiv electronic de ascultare în imediata apropiere a aparatului de cifrare aflat în ambasada Egiptului la Londra. Dându-se drept angajaţi ai companiei de telefonie veniţi să efectueze reparaţii, ofiţerii de informaţii britanici au putut să planteze într-un telefon din apropiere un dispozitiv capabil să detecteze clar sunetele care se auzeau când egiptenii configurau setările iniţiale ale aparatului. Cu aceste informaţii, spărgătorii de coduri britanici au putut să copieze setările respective pe propriul lor aparat, un model larg răspândit, şi spărgeau pe loc comunicaţiile egiptene cifrate. Operaţiuni asemănătoare au necesitat instalarea de dispozitive de supraveghere pe maşinile de scris electrice în timpul transportării lor la ambasada unei ţări.[70]

Progresele tehnologice din domeniul telecomunicaţiilor au ridicat noi probleme activităţii de culegere de informaţii prin interceptarea comunicaţiilor. În timp ce interceptarea transmisiilor radio tradiţionale depinde de capacitatea de a plasa o antenă de recepţie cu o sensibilitate rezonabilă în locaţia potrivită, iar interceptarea liniilor telefonice standard este o chestiune de obţinere a accesului fizic, interceptarea metodelor de comunicaţie mai noi ridică probleme mai mari. De exemplu, cablurile din fibră optică, adoptate pe scară largă întrucât asigură o lărgime de bandă mai mare (adică posibilitatea de a transmite mai multe informaţii pe unitate de timp) sunt, de asemenea, mai greu de interceptat decât cablurile pe care le înlocuiesc.[71] În mod asemănător, telefoanele celulare, în ciuda faptului că transmit pe unde radio, ridică probleme mari din cauza algoritmilor complecşi în funcţie de care sunt gestionate apelurile telefonice individuale în timp ce apelantul se deplasează dintr-o locaţie în alta.[72]

Activitatea de culegere de informaţii din telemetrie (Telint)

Celelalte forme de *sigint* sunt mai noi decât *comint*, iar ele reflectă utilizarea tot mai largă în domeniul militar a fenomenelor electromagnetice. Activitatea de culegere de informaţii din telemetrie sau *telint* este asemănătoare, ca şi concept, cu *comint*, cu excepţia faptului că respectivele comunicaţii care sunt interceptate au loc între un vehicul test (ca de exemplu o rachetă) şi o staţie aflată la sol şi nu constau în cuvinte, ci în indicaţiile primite de la diverşi senzori şi alte echipamente aflate la bord. (Aceste comunicaţii sunt cunoscute sub numele de telemetrie – "măsurare de la distanţă".) Valorile unor variabile ca acceleraţia vehiculului, temperatura în diverse puncte din interiorul vehiculului, consumul de carburanţi şi aşa mai departe, luate împreună, le oferă inginerilor aflaţi la sol o idee despre ce se întâmplă în vehiculul test. Acest lucru îi ajută pe ingineri să remedieze orice probleme care pot apărea în timpul testului şi să îmbunătăţească performanţa vehiculului.

În acelaşi timp, evident că astfel de informaţii sunt valoroase pentru potenţialii adversari. Dacă pot intercepta şi interpreta aceste fluxuri de date, vor obţine informaţii despre sisteme noi de armament când acestea sunt încă

la stadiul de test. (Analiza datelor de telemetrie este o sarcină foarte dificilă; împreună cu criptanaliza, este discutată în următorul capitol ca un tip de analiză a informațiilor secrete.) Astfel, la fel ca în cazul *comint*, țara care realizează testul poate încerca să le refuze altora accesul la informațiile telemetrice retransmițându-le către stațiile de la sol în formă criptată. O altă posibilitate este ca datele de telemetrie să fie înregistrate şi păstrate la bordul vehiculului test, urmând a fi recuperate şi extrase ulterior. Acest proces, numit "încapsulare", protejează datele împotriva interceptării; totuşi, poate fi o procedură riscantă, întrucât în cazul unei defecțiuni catastrofice a vehiculului test, exact când datele de telemetrie ar fi foarte utile, "capsula" care le conține poate fi distrusă sau greu de localizat.

Activitatea de culegere de informații prin mijloace electronice (Elint)

Activitatea de culegere de informații prin mijloace electronice sau *elint* presupune monitorizarea şi analizarea radiațiilor electromagnetice utilizate în alt scop decât cel al transmiterii unor mesaje şi care sunt emise de echipamentele militare străine. La bază, *elint* îi permite unei țări să urmărească elementele cheie ale forțelor armate aparținând unei alte țări (ca radarele sale antiaeriene, centrele de comandă şi control etc.), asigurând ceea ce este denumit uneori ca o "ordine electronică a conflictului". Sistemul EORSAT (Elint Ocean Reconnaisance Satellite – Satelit de recunoaştere maritim pentru culegerea de informații prin mijloace electronice) utilizat de fosta Uniune Sovietică, iar acum de Rusia, este un exemplu de astfel de monitorizare. Ani la rând, aceste dispozitive au fost folosite pentru a localiza şi a urmări navele de război americane prin interceptarea semnalelor electronice de rutină (ca de exemplu cele radar) emise de nave din largul mării.[73]

Cu toate acestea, activitatea de culegere de informații prin mijloace electronice nu presupune doar detectarea prezenței unui emițător. De exemplu, prin interceptarea unui semnal radar, se pot determina diverse caracteristici de funcționare ale radarului, ca de exemplu raza de acțiune (ce suprafață poate scana dintr-o dată) şi aria sa maximă de acoperire. De exemplu, aria de acoperire a unui radar care emite impulsuri individuale poate fi determinată din ritmul cu care se repetă impulsurile (numărul de impulsuri individuale sau "pachete" de unde radio emise pe secundă). Astfel, în timpul celui de Al Doilea Război Mondial serviciile secrete britanice au dedus din faptul că radarul antiaerian german Freya funcționa cu un ritm de repetare a impulsurilor de cinci sute de impulsuri pe secundă că raza sa maximă de acțiune este de trei sute de kilometri.[74]

Un caz mai recent care ilustrează valoarea pe care o are *elint* s-a manifestat în timpul ofensivei din 1982 a Israelului în Liban. În timp ce armata israeliană se deplasa pentru a elimina forțele Organizației de Eliberare a Palestinei (PLO) cu baza în Liban, un posibil atac din partea trupelor şi tancurilor siriene concentrate în Valea Bekaa din estul Libanului îngrijora înaltul comandament israelian. Protejarea acelor forțe era un atribut

al artileriei SAM siriene. Folosind aparate de zbor mici, fără pilot, cu viteză mică, israelienii au păcălit artileria siriană, determinând-o să îşi deschidă radarele de reglare a focului, deoarece aparatele de zbor emiteau semnalele unor avioane obişnuite; apoi, semnalele emise de forţele siriene erau înregistrate de un al doilea set de aparate de zbor israeliene. Pe baza acestor informaţii, israelienii au determinat caracteristicile operaţionale ale radarelor SAM şi le-au localizat. Drept urmare, în câteva ore, forţele aeriene israeliene au distrus aproape toată artileria siriană, au obţinut controlul incontestabil asupra spaţiului aerian al Libanului şi au eliminat orice posibilitate reală ca forţele siriene să intre în luptă de partea PLO.[75]

Activitatea de culegere de informaţii prin măsurători şi semnături (Masint)

Posibilităţile privind culegerea de informaţii din surse tehnice sunt limitate doar de legile fizicii şi ingeniozităţii umane. Pe lângă *photint* şi *sigint*, au mai fost folosite şi alte tehnici pentru a culege informaţii. Acestea au fost grupate împreună sub denumirea de culegere de informaţii prin măsurători şi semnături sau *masint*, deşi nu au prea multe în comun unele cu altele (în afară de faptul că nu sunt nici *photint*, nici *sigint*).[76]

De exemplu, s-au realizat senzori speciali care să detecteze şi să identifice caracteristicile detonărilor nucleare. Printre acestea se numără seismometrele, care măsoară undele de şoc asociate cu testele nucleare subterane; dispozitive pentru detectarea radioactivităţii asociate cu materiale nucleare sau căderile de pulberi radioactive din testele nucleare realizate la suprafaţă; şi senzori pentru detectarea de la distanţă a fasciculelor de lumină produse de testele nucleare realizate la suprafaţă.[77] Un alt tip de senzor, sonarul, utilizează un alt fenomen natural, undele sonore, pentru a detecta submarinele aflate în misiune. În afară de locaţia submarinului, pot fi determinate şi alte caracteristici ale acestuia în urma unei analize a sunetelor pe care le emite sau le reflectă.[78]

Platforme pentru culegerea de informaţii

În dezbaterile publice şi în studiul nostru, s-a pus accentul pe culegerea de informaţii prin sisteme bazate pe sateliţi. În mod evident, sateliţii au avantajul de a survola orice parte de lume, fără a ţine cont de graniţele internaţionale.[79] Din acest motiv, sunt extrem de valoroase pentru culegerea de informaţii din ţări în care accesul este imposibil din cauza izolării lor şi a măsurilor stricte de securitate. Cu toate acestea, au şi anumite dezavantaje:

- Sunt, în general, mai scumpe decât alte platforme de recunoaştere.[80]
- Nu se pot apropia foarte mult de ţintele lor (în general, sateliţii aflaţi mai jos pe orbita pământului rămân la altitudini cu mult peste o sută de mile, în timp ce sateliţii din orbita geostaţionară trebuie să se situeze la o altitudine de 22.400 de mile).

- Sunt relativ inutili o mare parte din timp, chiar dacă orbitele lor sunt calculate pentru a maximiza informaţiile pe care le culeg (cu alte cuvinte, un satelit de recunoaştere fotografică care prin fotografiile pe care le face în Rusia sau Orientul Mijlociu justifică investiţia realizată, trebuie, totuşi, conform legilor fizicii orbitale, să petreacă perioade îndelungate în Emisfera Sudică într-un mod mai puţin eficient).
- Orbitele lor sunt previzibile, deci inamicul poate să îşi avertizeze trupele şi echipamentele sensibile cu privire la momentul în care vor fi vulnerabile faţă de activitatea de observare efectuată de un satelit de recunoaştere.[81]

Astfel, deşi activitatea de recunoaştere spaţială prezintă numeroase şi importante avantaje, există şi alte tipuri de platforme care continuă să joace roluri semnificative în sfera exploatării tehnice. Avioanele, de exemplu, pot efectua misiuni la periferia teritoriului unui adversar; pot intercepta comunicaţii care nu pot fi interceptate din spaţiu; pot fotografia zone aflate în apropierea graniţelor teritoriale, rămânând în acelaşi timp în siguranţă în afara spaţiului aerian al ţării ţintă; şi pot intercepta semnalele radar provenite de la radarele antiaeriene ale adversarului, care ar fi putut fi activate tocmai în scopul identificării traiectoriei avionului. Aparatele de zbor fără pilot (vehicule aeriene fără echipaj sau UAV-uri) pot fi utilizate în zone în care mijloacele de apărare antiaeriene inamice prezintă un risc extrem de mare pentru piloţi şi echipajele vehiculelor. Aparatele de zbor au multe avantaje (care corespund dezavantajelor prezentate în cazul sateliţilor): sunt mai ieftine decât sateliţii, se pot apropia mai mult de ţintele lor, pot plana deasupra zonelor de interes şi, poate cel mai important, traiectoriile lor nu pot fi anticipate.

În Războiul din Golf din 1990-91, avioanele de supraveghere AWACS (Airborne Warning and Control System – Sistem aeropurtat de avertizare şi control) şi J-STARS (Joint Surveillance Target Attack Radar System – Sistem radar de supraveghere comună pentru atacarea ţintelor) care zburau în spatele liniilor americane le-au permis comandanţilor americani să urmărească şi să ţintească mişcările de trupe şi aparate de zbor irakiene aproape în timp real. În special J-STARS a oferit date critice despre dispunerea forţelor terestre irakiene cu puţin timp înainte de începerea ofensivei declanşate de coaliţie, reasigurând coaliţia că manevra sa surpriză din jurul flancului drept al inamicului nu va întâmpina, practic, nici un fel de rezistenţă. În timpul Bătăliei de la Al-Khafji, în data de 29 ianuarie 1991, J-STARS a detectat un convoi irakian de forţe de urmărire care se deplasau înspre sud din Kuwait City. Aceste informaţii au fost transmise imediat comandanţilor coaliţiei, care au ordonat atacuri aeriene împotriva trupelor irakiene care înaintau. În câteva ore, au fost distruse cincizeci şi opt din cele şaizeci şi una de vehicule ale convoiului.[82]

La operaţiunea NATO din Kosovo din 1999 (Operaţiunea Forţa Aliată) s-a înregistrat o utilizare "fără precedent" de UAV-uri în scop de

recunoaştere, "reducându-se necesitatea de a trimite aparate de zbor cu echipaj în spaţiul aerian ostil."[83] Flexibilitatea UAV-urilor a fost reliefată în următoarea observaţie făcută de înalţii oficiali ai SUA: "Deşi s-a pierdut un număr semnificativ de UAV-uri, capacitatea lor de a se deplasa deasupra unui teritoriu ostil le-a permis să ofere informaţii din activitatea de supraveghere, care nu puteau fi obţinute prin alte mijloace, şi a eliminat riscul de a pierde echipaje. Mai mult, în proiectarea UAV-urilor s-a urmărit o singură utilizare a acestora, obţinerea unui cost redus fiind prioritară faţă de durata de viaţă a aparatului."

Pe lângă aparatele de zbor, şi alte platforme pot fi utile pentru culegerea de informaţii din surse tehnice. Furgonetele şi camioanele pot monitoriza în mod clandestin comunicaţiile şi semnalele echipamentelor militare, diplomatice sau ştiinţifice în timp ce stau parcate în apropiere. În mod asemănător, navele pot intercepta semnalele radio de pe coasta unui inamic. Radarele maritime sau terestre, dacă pot fi amplasate suficient de aproape de o locaţie de unde se lansează proiectile test sau unde focoasele reintră în atmosfera pământului, pot să urmărească testele de zbor cu proiectile ale unui inamic şi să determine unele dintre caracteristicile rachetei. Locaţiile aflate la sol, în funcţie de amplasare, pot, de asemenea, să fie utilizate pentru a intercepta diverse semnale radio, inclusiv semnale care este posibil să fi ricoşat accidental de pe suprafaţa lunii.[84] În sfârşit, reducerea dimensiunilor dispozitivelor de ascultare şi a altor senzori le permite serviciilor de informaţii să culeagă informaţii din surse tehnice atunci când un agent poate să se apropie suficient de ţintă şi să "planteze" senzorul pe ascuns.[85]

Pe scurt, caracterul platformelor pentru culegerea de informaţii poate varia de la obişnuit la exotic. Pentru o comunitate de informaţii modernă, avansată din punct de vedere tehnologic, decizia privind ce platforme să se folosească şi în ce combinaţii este, în primul rând, rezultatul a două evaluări: Ce platforme pot culege cel mai bine informaţiile dorite? În al doilea rând, care sunt costurile şi riscurile aferente pe care le implică utilizarea anumitor platforme?

COMPARAŢIE ÎNTRE HUMINT ŞI TECHINT

De-a lungul anilor, a existat o dezbatere continuă în Statele Unite cu privire la importanţa pe care o au *humint* şi *techint*. Pe de o parte, sunt cei care consideră culegerea de informaţii din surse tehnice ca fiind primordială şi că având probabilitatea de a continua să îşi sporească însemnătatea rolului său pe măsură ce tehnologia progresează; pe de altă parte, sunt cei care cred că importanţa culegerii de informaţii din surse tehnice a fost exagerată, în detrimentul spionajului tradiţional, şi că trebuie restabilit acest echilibru.

O contribuţie remarcabilă la această dezbatere a fost apărarea îndrăzneaţă a întâietăţii *techint* din memoriile amiralului Stansfield Turner, directorul CIA din timpul mandatului preşedintelui Carter:

> Acum, când avem sisteme tehnice, care variază de la sateliți ce călătoresc în spațiu pe tot globul până la aparate de zbor care ajung în spațiul aerian internațional, la senzori în miniatură amplasați pe ascuns în apropierea unor ținte dificile, nu suntem departe de momentul în care vom supraveghea aproape orice punct de pe suprafața pământului cu un senzor și probabil că nu doar cu unul singur. Putem să facem fotografii detaliate de la distanțe foarte mari, să detectăm sursele de căldură prin dispozitive cu infraroșu, să localizăm cu exactitate metalul cu detectoare magnetice, să facem diferența între obiecte care abia se mișcă și unele imobile cu ajutorul radarelor Doppler, să folosim radarul pentru a detecta obiecte care sunt acoperite sau ascunse în întuneric, să interceptăm prin toate mijloacele semnale de la vocea umană la unde radio electronice, să detectăm radiația nucleară cu contoare Geiger exacte și să înregistrăm explozii subterane la distanțe mari cu ajutorul dispozitivelor seismice. Majoritatea activităților pe care intenționăm să le monitorizăm implică emiterea unor semnale diferite. În conflict, tancurile pot fi detectate după căldura ce provine de la motoare, după magnetismul blindajului sau prin fotografiere. O fabrică de arme nucleare emite radiații, are o formă fizică exterioară aparte și este alimentată cu anumite tipuri de materiale. Într-un fel sau altul, ar trebui ca în curând să putem să urmărim majoritatea activităților de pe suprafața pământului, zi și noapte, pe vreme bună sau rea.[86]

Curajul tehnologic absolut implicat în crearea acestor tipuri de dispozitive pentru culegerea de informații din surse tehnice este, într-adevăr, extraordinar. Cu toate acestea, admirația față de tehnologie poate să conducă ușor la o supraestimare a ceea ce poate realiza *techint* și la o subestimare concomitentă a activității de culegere de informații din surse umane (*humint*). În Statele Unite, această perspectivă a fost predominantă în special la mijlocul și la sfârșitul anilor 1970; cu toate acestea, de atunci, importanța *humint* a primit o nouă recunoaștere.

Avantajele *techint* sunt descrise foarte bine în pasajul citat mai sus. Activitatea de culegere de informații din surse tehnice a fost indispensabilă în Statele Unite pentru culegerea majorității informațiilor pe care le-a obținut despre Uniunea Sovietică. Cu toate acestea, trebuie remarcat că, în multe alte țări, o mare parte a acestor informații sunt disponibile în mod public. Informații despre mărimea și structura generală a forțelor armate și despre dezvoltarea unor importante sisteme de armament noi, de exemplu, sunt disponibile în majoritatea țărilor în documente oficiale (în special bugetare și parlamentare). Cu toate acestea, au fost necesare metode complexe și costisitoare de exploatare tehnică pentru a culege aceste informații despre Uniunea Sovietică, din cauza caracterului secret pe care regimul îl conferă aspectelor militare în special și celor ce țin de securitatea națională în general. O mare parte din activitatea de culegere de informații din surse

tehnice, care s-a realizat de-a lungul anilor, a fost îndreptată către contracararea efectelor acestui caracter secret.

Cu toate acestea, de la prăbuşirea Uniunii Sovietice şi dizolvarea Pactului de la Varşovia, numărul "ţintelor dificile" s-a redus substanţial şi, odată cu acesta, şi necesitatea de a acorda o pondere atât de mare culegerii de informaţii din surse tehnice. Bineînţeles, încă există societăţi închise, iar unele dintre ele, cum ar fi Coreea de Nord, prezintă un interes major pentru activitatea de culegere de informaţii; în acest caz, probabil că va continua tendinţa de a acorda o importanţă mare *techint*. Un caz mai interesant ar fi cel al Republicii Populare Chineze, ce rămâne o ţară în care spionajul se realizează cu dificultate, dar care este mult mai deschisă în ceea ce priveşte libera circulaţie şi comunicaţiile decât a fost vreodată Uniunea Sovietică.

Mai mult, în ceea ce priveşte o mare parte din categoriile de informaţii pe care toate ţările le păstrează secrete – cum ar fi intenţiile şi planurile politice şi militare – culegerea de informaţii din surse umane a fost întotdeauna, şi încă este, necesară. Partizanii *humint* subliniază că, în ciuda progresului tehnologic, spionajul tradiţional este în continuare necesar pentru a furniza informaţii despre intenţiile, activitatea politică şi conceptele strategice ale conducerii unei ţări inamice. Culegerea de informaţii din surse tehnice, de exemplu, a demonstrat clar comasarea armatei irakiene la graniţa kuwaitiană în iulie 1990; ceea ce nu a putut elucida a fost intenţia lui Saddam Hussein: Voia să invadeze Kuwaitul sau să impună adoptarea unor concesii financiare? În schimb, un agent bine plasat din statul major al armatei poloneze a informat cu privire la decizia secretă a guvernului polonez din 1981 de a impune legea marţială pentru a zdrobi Solidaritatea, mişcarea sindicalistă independentă.[87] Pe scurt, înţelegerea intenţiilor inamicului, a strategiei sale şi a percepţiei pe care o are cu privire la situaţia în care se află este, deseori, cea mai de preţ informaţie pe care o putem avea.

Interceptarea comunicaţiilor dintre conducerea politică şi cea militară a ţării inamice (*comint* la nivel înalt) poate oferi, de asemenea, informaţii de acest tip; este ca şi cum ai avea un agent cu acces nelimitat la liderii inamici. Totuşi, obţinerea acestor informaţii prin *comint* este mult mai dificilă decât lasă să se vadă expunerea lui Turner. În primul rând, se poate presupune că un adversar îşi criptează majoritatea comunicaţiilor sensibile. În această ordine de idei, trebuie remarcat faptul că activitatea de culegere de informaţii din surse umane poate fi utilă şi chiar critică şi în această privinţă: poate oferi liste de coduri sau alte informaţii care facilitează decriptarea mesajelor. De exemplu, la începutul anilor 1930, serviciile de informaţii franceze au obţinut de la un agent din Germania informaţii importante despre aparatul de codare german numit "Enigma", inclusiv instrucţiuni pentru întrebuinţarea sa, unele detalii despre construcţia sa şi "cheile" care specificau modul în care trebuia configurat aparatul zilnic. Aceste informaţii au fost împărtăşite serviciului de informaţii polonez, care a realizat progrese criptanalitice majore, ce au stat la baza succesului pe care Marea Britanie l-a avut cu Ultra în timpul celui de Al Doilea Război Mondial.[88]

În al doilea rând, majoritatea mijloacelor *comint* pot fi combătute transmiţând mesajele, nu pe calea aerului, ci prin cablu. Interceptarea comunicaţiilor prin "mijloace fixe" necesită obţinerea accesului la cabluri, ceea ce este un lucru dificil în majoritatea cazurilor. Mai mult, după cum am menţionat deja, cablurile tradiţionale sunt înlocuite cu cabluri din fibră optică, ce utilizează lumina coerentă (raze laser) pentru a transmite mesajele şi sunt mult mai puţin vulnerabile la interceptare.

În plus, toate tipurile de mijloace tehnologice de culegere de informaţii, inclusiv *comint*, suferă de un posibil "impediment al banilor". Având în vedere răspândirea globală a sistemelor de culegere de informaţii din surse tehnice, trebuie să existe o metodă prin care să li se comande ce ţinte să supravegheze şi pe care să le ignore.[89] Deşi poate fi adevărat că "[în curând] vom putea supraveghea aproape orice punct de pe suprafaţa pământului cu un senzor", nimeni nu ar putea să le supravegheze pe toate în acelaşi timp şi, chiar dacă ar putea, i-ar fi imposibil să proceseze şi să analizeze toate datele pe care le-ar culege senzorii.

Astfel, existenţa posibilităţilor tehnice, ca cele descrise de Turner, înseamnă că aspecte importante la nivel mondial pot trece neobservate de un serviciu de informaţii bine echipat. După cum a devenit evident în urma inspecţiilor întreprinse după Războiul din Golf, culegerea de informaţii din surse tehnice de către americani înainte de război nu a fost suficientă pentru a urmări încercarea Irakului de a construi o armă nucleară.[90] Problema nu se pune dacă activitatea de culegere de informaţii din surse tehnice este valoroasă. Pur şi simplu, pământul este un loc cuprinzător, variat şi, în unele zone, foarte activ. În consecinţă, multe depind de capacitatea de a amplasa senzorii în mod corespunzător. Culegerea de informaţii din surse umane poate oferi primul indiciu esenţial că se întâmplă ceva de interes sau că se va întâmpla la o locaţie dată. Acest lucru face posibilă îndreptarea sistemelor tehnice asupra zonei respective. Fără aceste indicii, sistemele ar fi mai puţin eficiente şi ar putea rata evenimente importante fie pe perioade lungi de timp, fie în întregime.

O sursă umană de informaţii poate oferi şi indiciile necesare pentru interpretarea datelor brute strânse de un sistem de culegere de informaţii din surse tehnice. Chiar şi cu o fotografie clară a unei clădiri, de exemplu, este posibil ca un expert dintr-un serviciu de informaţii să nu îi poată identifica ce tip de activităţi se desfăşoară în acea locaţie. Cu toate acestea, o sursă umană cunoscătoare poate să explice că prezenţa unui anumit detaliu, care altfel nu se remarcă, indică faptul că respectiva clădire a fost proiectată cu un anumit scop, legat de un anumit program militar. Fără sursa umană, este posibil ca detaliul să nu fie observat sau semnificaţia să nu fie înţeleasă. Dar, odată ce această "semnătură" este recunoscută, pot fi examinate fotografii ale unor clădiri asemănătoare pentru a vedea dacă este prezent acelaşi detaliu.

Totuşi, în mai multe cazuri, semnăturile posibilelor ţinte ale culegerii de informaţii sunt din ce în ce mai greu de identificat sau, dacă sunt identificabile, sunt greu de urmărit. Uneori, acest lucru se întâmplă deoarece ţintele au devenit mai mici, mai mobile sau au devenit subterane. Alteori,

cauza o reprezintă faptul că activitatea care este de interes pentru serviciile de informații (cum ar fi cercetarea în domeniul armelor biologice sau chimice) nu se poate distinge rapid de activitățile conexe, dar legale (ca de exemplu fabricarea de produse farmaceutice sau pesticide). În plus, în unele cazuri poate fi posibil să se elimine în totalitate semnăturile cheie care oferă indicii. După Războiul din Golf, de exemplu, echipa ONU trimisă în Irak pentru a găsi şi a distruge facilitățile de arme nucleare din această țară a descoperit că Irakul construise cu minuțiozitate multe dintre clădirile din program pentru a evita detectarea cu ajutorul sateliților şi al altor sisteme tehnice de culegere de informații. Unele fuseseră construite pentru a împiedica emisiile radioactive, în timp ce altele fuseseră proiectate pentru a atrage cât mai puțin atenția asupra lor, imitând înfățişarea fabricilor industriale legale. Se pare că abia după ce un inginer irakian care cunoştea încercarea lui Saddam Hussein de a construi o bombă a trecut de partea adversă după război au fost identificate aceste locații ca făcând parte din programul Irakului de dezvoltare a armelor nucleare.[91]

Totuşi, în ceea ce priveşte unele tipuri de informații secrete, problema legată de identificarea în mod corect a țintelor de către sistemele tehnice de culegere de informații poate fi aproape imposibil de rezolvat. De exemplu, este posibil ca *humint* să fie necesar pentru a culege informații cruciale despre ținte nonguvernamentale (cum ar fi organizații teroriste) care nu dețin locații stabile sau rețele de comunicații ce pot fi exploatate din punct de vedere tehnic. Altfel spus, cu cât o grupare poate fi asociată cu mai puține locații cunoscute, cu atât este mai greu de îndreptat senzorii tehnici asupra lor. Culegerea de informații despre astfel de grupări poate depinde foarte mult de capacitatea de infiltrare în grupare sau de recrutare a membrilor săi ca informatori. Dacă grupările de acest tip devin ținte importante ale serviciilor de informații, culegerea de informații din surse umane va deveni, la rândul ei, mai importantă.

Prin urmare, *humint* şi *techint* pot avea roluri complementare; separat, pot oferi diverse tipuri de informații. Bineînțeles că prăbuşirea "Cortinei de Fier" a eliminat motivul inițial care a stat la baza dezvoltării de către Statele Unite a unui sistem sofisticat de exploatare tehnică. Cu toate acestea, obligațiile continue de a monitoriza depozitele de arme ale altor state, în special ale statelor cu societăți închise şi programe active de dezvoltare a armelor de distrugere în masă, împreună cu o cerere din ce în ce mai mare de informații tehnice din partea armatei americane pentru sprijinirea operațiunilor sale sugerează că este puțin probabilă o îndepărtare substanțială de activitatea de culegere de informații din surse tehnice. Pe de altă parte, necesitatea culegerii de informații despre state noi, actori politici noi şi preocupări noi este satisfăcută cel mai bine de culegerea de informații din surse umane. Deşi amestecul corect de *humint* şi *techint* va fi, aşa cum a fost şi în trecut, un subiect dezbătut pe larg, este foarte probabil ca o putere globală ca Statele Unite să continue să aibă nevoie de amândouă.

Această discuție despre *humint* şi *techint* a abordat importanța fiecăreia pentru culegerea de informații strategice – informații destinate

factorilor de decizie la nivel național. De asemenea, este, totuși, important de remarcat că progresele din telecomunicații și IT au făcut posibil ca informațiile culese de sistemele *techint* (inclusiv cele dezvoltate pentru a fi utilizate la nivel național) să fie puse la dispoziția comandanților pe câmpul de luptă în timp real – sau, în orice caz, suficient de rapid pentru a fi utile în scop tactic. Această dezvoltare se află încă la început, dar promite să devină o utilizare importantă dată sistemelor *techint*.[92]

CULEGEREA DE INFORMAȚII DIN SURSE DESCHISE

Publicații și emisiuni radio și TV

Nici o discuție despre culegerea de informații nu ar fi completă dacă nu s-ar face referire la strângerea de informații din surse deschise – adică ziare, cărți, emisiuni radio și de televiziune, internet și orice altă sursă publică de informații.

Importanța surselor deschise în procesul culegerii de informații este un subiect de dezbatere și, în fond, este legată de aspecte fundamentale privind categoria informațiilor. O perspectivă, exemplificată de Sherman Kent, este că majoritatea "activităților de culegere de informații externe eficiente de la nivel înalt... trebuie să se realizeze prin observație și cercetare deschisă, directă și realistă."[93] Pe de altă parte, perspectiva mai tradițională este că, deși sursele deschise pot oferi un context și o bază importante, faptele cheie, cum ar fi intențiile exacte ale unui inamic, trebuie obținute în primul rând, dacă nu exclusiv, din surse care nu sunt publice, apelându-se la spionaj sau exploatare tehnică.

Această problemă este discutată pe larg în capitolul 7. În acest moment, accentul se va pune pe diversele întrebuințări care le pot fi date informațiilor din surse deschise. De exemplu, o sarcină standard a ofițerilor din serviciile de informații a fost să pregătească compendii extinse cu informații privind țările în care ar putea fi întreprinse operațiuni militare în viitor. Teoretic, aceste compendii includ toate informațiile care ar putea fi utile personalului militar. Informații privind geografia țării, rețelele sale de comunicații și transport, locații militare și economice cheie și așa mai departe ar trebui incluse cu detalii suficiente pentru a permite celui care elaborează planul să ia o serie largă de decizii, ca de exemplu să determine cât de repede ar putea fi mutate trupele și proviziile din punctul A în punctul B.

Cu excepția celor mai secretoase țări (cum ar fi fosta Uniunea Sovietică, ce a recunoscut în 1988 că a falsificat hărți ca măsură de securitate),[94] o mare parte din aceste informații vor fi disponibile în literatura surselor deschise: hărți și orare rutiere și feroviare, articole din ziare și reviste, rapoarte economice și statistice ale guvernului și chiar ghiduri de călătorie vechi. Culegerea și catalogarea lor reprezintă alte aspecte. Sunt implicate volume uriașe de informații, și este puțin probabil să fie disponibile vreodată resursele necesare culegerii lor pentru fiecare țară în

parte. Dacă, după cum vom discuta în următorul capitol, forţei militare americane care a invadat Grenada în 1983 nu i-au fost furnizate hărţi corespunzătoare şi alte informaţii despre insulă, motivul nu l-a reprezentat dificultatea de a culege informaţii, ci nealocarea unor resurse suficiente pentru ceea ce probabil că multora li s-a părut a fi o insulă mică, îndepărtată.

În mod asemănător, o gamă largă de surse statistice din toată lumea fac publice date economice. Cu toate acestea, pentru a hotărî ce date trebuie culese trebuie să ştii ce informaţii sunt necesare. Este posibil să fie nevoie de date economice pentru a susţine formularea politicii privind comerţul internaţional sau sancţiunile economice, a face faţă efectelor crizelor şi cartelelor internaţionale (cum ar fi Organizaţia Ţărilor Exportatoare de Petrol) şi aşa mai departe. Alte tipuri de date economice, ca de exemplu cele care ar rezulta din monitorizarea circuitelor financiare, ar putea face lumină asupra traficului internaţional de droguri. În sfârşit, este posibil să fie nevoie de culegerea de informaţii economice pentru a susţine analizele politice şi militare. De exemplu, în timpul celui de Al Doilea Război Mondial, economiştii de la Biroul de Servicii Strategice sau OSS (care lucrau pentru forţele aeriene americane din Europa) au folosit o gamă largă de date economice, în mare măsură neclasificate, pentru a contribui la planificarea unei campanii strategice de bombardament; obiectivul a fost distrugerea părţilor din infrastructura industrială germană – ca uzinele petroliere şi de rulmenţi – considerate vitale pentru sprijinirea succesului războiului nazist.[95] În vremurile mai recente, prezicerile privind comportamentul sovieticilor la sfârşitul anilor 1980 au fost dominate de întrebări legate de modul în care va afecta această situaţie economică alte domenii strategice. Fiecare dintre aceste necesităţii privind culegerea de informaţii atrage după sine diferite categorii de date economice.

Pe lângă aceste tipuri evidente de materiale din surse deschise, analiştii serviciilor de informaţii solicită aceleaşi genuri de informaţii – discursuri ale unor figuri politice proeminente, texte de lege şi rezoluţii, recensăminte şi alte date demografice – care ar fi necesare pentru orice analiză academică a condiţiilor politice sau sociale dintr-o ţară străină; într-adevăr, produsul final poate fi asemănător.

În funcţie de resursele disponibile, un serviciu de informaţii poate culege datele specializate în cantităţi care ar copleşi un cercetător universitar. De exemplu, o tehnică importantă pentru a înţelege politicile şi procesele de stabilire a strategiilor în sistemele politice "închise" presupune urmărirea carierei unui număr mare de indivizi pentru a identifica ce oficiali de nivel mediu sunt protejaţii sau "clienţii" căror lideri. După ce au fost identificate aceste relaţii patron-client, un analist poate, observând promovările şi retrogradările clienţilor, să determine poziţia adoptată de protectorii lor de nivel înalt. A face acest lucru, totuşi, necesită strângerea şi păstrarea unei vaste baze de date biografice. Ar presupune parcurgerea tuturor ziarelor importante şi a tuturor emisiunilor de ştiri; înregistrarea fiecărei ştiri care indică promovarea, retrogradarea sau transferarea unui oficial sau care stabileşte legătura între doi oficiali; şi introducerea în computer a bazei de date rezultate, astfel încât să devină utilă pentru specialişti. Unui om de

ştiinţă, chiar şi unui institut de învăţământ superior, s-ar putea să îi fie greu să întreprindă o astfel de sarcină.[96]

Informarea realizată de diplomaţi şi ataşaţi militari

Un alt mijloc de culegere a informaţiilor – unul care ar putea fi considerat un amestec de *humint* şi sursă deschisă, deoarece este obţinut de agenţi, dar într-un mod direct şi deschis – ar fi rapoartele pe care le prezintă diplomaţii şi ataşaţii militari cu privire la evenimente din ţările în care sunt numiţi la post. Într-adevăr, linia de demarcaţie dintre diplomat şi ofiţer de informaţii nu a fost niciodată clară. După cum afirmă un istoric al diplomaţiei: "Uneori, ambasadorii au traversat rapid graniţa confuză dintre culegerea legitimă de informaţii şi spionaj şi alte activităţi cu o reputaţie proastă."[97] Dar chiar şi astăzi, când cele două funcţii sunt separate, rapoartele diplomatice despre situaţia politică din ţara gazdă pot reprezenta informaţii importante pentru orice analiză politică. Un diplomat care beneficiază de un acces considerabil la figurile politice majore dintr-o ţară sau este un fin cunoscător al istoriei ţării şi al structurii politice ar trebui să poată să ofere o evaluare a situaţiei politice interne, care nu se poate regăsi în mass media.[98]

În mod asemănător, ataşaţii militari, în măsura în care au acces la ofiţeri din ţara gazdă, pot cunoaşte îndeaproape sistemul militar al statului respectiv, ca de exemplu personalitatea şi competenţa ofiţerilor de rang înalt, precum şi modul lor de gândire caracteristic, punctele lor de vedere privind doctrina militară şi relaţiile cu conducerea civilă. În plus, ataşaţii pot fi invitaţi să urmărească exerciţii militare sau să ia parte la demonstraţii sau ocazii ceremoniale la care defilează sau zboară echipamente militare. De asemenea, pot să călătorească în ţara gazdă şi, astfel, să vadă aerodromuri, porturi şi alte baze militare şi civile de interes.[99]

Alte surse umane nesecrete

Diplomaţii şi ataşaţii militari nu sunt singurii cetăţeni străini care vizitează ţări şi raportează observaţiile lor. De exemplu, acordul din 1987 încheiat între Statele Unite şi URSS privind eliminarea rachetelor cu rază medie şi scurtă de acţiune (Tratatul INF) şi, mai recent, Tratatul de Reducere a Armelor Strategice (START) prevăd ca fiecare parte să trimită inspectori la anumite baze militare ale celeilalte părţi pentru a constata dacă ţara respectivă respectă termenii tratatului. Inspectorii au un acces mai mare la acele baze decât ar avea ataşaţii militari sau alţi vizitatori. Evident, rapoartele lor vor conţine informaţii valoroase privind forţele militare ale ţării gazdă.

În mod asemănător, oamenii de afaceri, savanţii şi alte persoane care călătoresc află informaţii despre ţările pe care le vizitează – informaţii care, deşi nu sunt secrete în mod oficial, nu sunt disponibile în mod public. Ca aceste informaţii să ajungă la guvernul ţării lor este necesar, într-o ţară ai cărei cetăţeni nu au nevoie de o permisiune specială pentru a călători în străinătate, ca aceste persoane să fie dispuse să le transmită. Dar intensificarea generală a comerţului internaţional, turismului şi cercetării a însemnat o dezvoltare substanţială în ultimii ani a posibilităţilor privind culegerea de informaţii din surse umane nesecrete.

Capitolul 3

CE ÎNSEAMNĂ TOATE ACESTEA? ANALIZA ŞI PRODUCEREA INFORMAȚIILOR

CE ESTE ANALIZA?

Analiza se referă la procesul de transformare a informațiilor care sunt culese în orice mod într-un produs care poate fi folosit de factorii de decizie şi liderii militari. Rezultatul sau "produsul informațional" poate lua forma unor scurte memorandumuri, rapoarte oficiale amănunțite, expuneri sau orice alte mijloace de prezentare a informațiilor. Această secțiune arată gama de tehnici analitice. La descrierea acestor activități, nu este utilizată întotdeauna terminologia standard a activității de informații; mai mult decât atât, analiza nu are categorii standard. În plus, categoriile care există nu sunt nici exacte, nici nu se exclud reciproc. Aici s-a încercat să se aranjeze tehnicile de la cea mai tehnică, precum decriptarea mesajelor, la cea mai speculativă, ca de exemplu prezicerea viitoarelor tendințe sociale şi politice. Într-o secțiune ulterioară se discută despre diversitatea de produse informaționale şi funcțiile pe care le îndeplinesc.

Analiza tehnică

Utilizăm termenul de "analiză tehnică" aici pentru a ne referi la metodele analitice care transformă datele foarte specializate, total sau aproape de neînțeles pentru oricine altcineva în afară de specialist, în date pe care le pot folosi alți analişti din domeniul informațiilor. Exemplele discutate sunt criptanaliza (care transformă şiruri aparent aleatorii de litere şi numere într-un mesaj într-un limbă cunoscută), analiza telemetrică (ce transformă un semnal radio într-o serie de valori care descriu capacitatea de zbor a unei rachete sau a unui alt vehicul de testare) şi interpretarea fotografică (ce identifică şi măsoară obiectele dintr-o fotografie).

Criptanaliza. Criptanaliza se referă la rezolvarea sau "spargerea" codurilor şi cifrurilor inamice, prin aceasta permițându-le analiştilor să transforme un mesaj criptat interceptat în forma lui inițială, cu înțeles. În majoritatea cazurilor, interceptarea presupunea receptarea unor semnale radio de către altcineva decât destinatarul lor. Cu toate acestea, problema criptanalitică este aceeaşi în cazul unui mesaj criptat luat de la un curier capturat, o scrisoare criptată deschisă de cenzura poştală sau o telegramă criptată obținută prin interceptarea cablului telegrafic.

În uzajul tehnic, termenii *cod* şi *cifru* se referă la metode diferite de criptare. Într-un cod, un cuvânt sau o expresie (care semnifică un lucru, un concept sau o locație) sunt înlocuite cu un grup de cifre sau litere (care pot

sau nu să formeze un cuvânt real) ce se găseşte opus cuvântului sau expresiei respective într-o listă de coduri. Astfel, mesajul "Attack on Saturday" (Atac sâmbătă) s-ar cripta prin găsirea grupului de coduri pentru "attack" (să spunem FGHJ) şi al celui pentru "Saturday" (să spunem ADFK), producând astfel mesajul criptat FGHJ ADFK. Dacă un cuvânt nu se găseşte în lista de coduri, expeditorul poate fie să reformuleze mesajul pentru a utiliza cuvinte şi expresii care apar în ea, fie să exprime literă cu literă cuvântul lipsă folosind grupuri speciale de coduri pentru litere sau silabe individuale.

Pe de altă parte, într-un cifru, fiecare literă din mesajul inițial – numit *text lizibil* – este înlocuit, urmând o formulă sau un algoritm, cu o altă literă, formând astfel *textul cifrat*. (Într-un cifru "de transpunere", literele mesajului original sunt păstrate, dar sunt transmise într-o ordine aleatorie, conform unei scheme.) De exemplu, un cifru ar putea consta din regula conform căreia fiecare literă să fie înlocuită cu litera care o urmează în alfabet. În acest cifru extrem de simplu, mesajul din exemplul dat mai sus ar fi cifrat ca BUUBDL PO TBUVSEBZ.

Un cifru mai complicat (dar mult prea simplu pentru a oferi siguranță) ar putea consta din următorul algoritm: se înlocuieşte prima literă din mesaj cu litera care o urmează în alfabet; a doua literă, cu litera care se află cu două poziții mai jos în alfabet; şi aşa mai departe. (În cazul unui astfel de cifru, alfabetul ar fi considerat scris într-un cerc, cu litera A urmându-i imediat literei Z. Astfel, cea de a douăzeci şi şasea literă a mesajului ar fi neschimbată, în timp ce cea de a douăzeci şi şaptea, la fel ca prima, ar fi înlocuită cu cea care îi urmează imediat şi aşa mai departe.) Acum, mesajul ar fi BVWEHQ VV BKEGERPO.

Aceste tehnici pot fi combinate în diverse moduri. De exemplu, un mesaj codat poate fi el însuşi cifrat în acelaşi mod în care ar putea fi şi un text lizibil. Astfel, mesajul pe care l-am dat drept exemplu – codat ca mai înainte şi apoi cifrat cu prima metodă discutată – ar genera următorul text "supercifrat": GHIK BEGL. Avantajul unei astfel de proceduri este securitatea sporită pe care o oferă: Pentru a recupera mesajul original, un inamic trebuie să spargă atât codul, cât şi cifrul. De obicei, codul rămâne valabil mult timp, în timp ce algoritmul cifrului se schimbă frecvent. Motivul este acela că, în timp ce primul este destul de greu de schimbat (fiecare schimbare de cod înseamnă că trebuie distribuite noi liste de coduri fiecărei ambasade, baze sau poşte care ar putea trimite sau primi mesaje), algoritmul cifrului este simplu de schimbat.

Criptanaliza este procesul de rezolvare ("spargere") a codurilor şi a cifrurilor – adică, reconstituirea listei de coduri a inamicului sau descoperirea metodei acestuia de cifrare a mesajelor – folosind, în primul rând, chiar mesajele criptate. (*Decriptarea*, pe de altă parte, se referă de obicei la procesul prin care destinatarul – care, bineînțeles că ştie deja codul sau cifrul folosite – recuperează textul inițial.) *Criptologia* este studiul mai general al acestor aspecte, atât în scopuri criptanalitice, cât şi în scopurile realizării unor coduri şi cifruri mai sigure. *Criptografia* se referă uneori la

activitatea de realizare a codurilor şi a cifrurilor, dar este folosită câteodată şi ca sinonim pentru criptologie.

Materia primă cu care începe de obicei criptanaliza este o colecţie de mesaje criptate. Sarcina criptanalizei este de a identifica tiparele existente în amalgamul de litere şi cifre, aparent fără sens, şi de a stabili legătura între acele tipare şi tiparele cunoscute, existente în limba în care se presupune că au fost scrise mesajele. De exemplu, în textele obişnuite în limba engleză, litera E este mai frecventă decât oricare alta; aşadar, într-un grup de mesaje cifrate folosind metoda simplă de substituţie, despre care am discutat mai sus (în care fiecare literă din textul iniţial este înlocuită cu cea care o urmează imediat în alfabet), litera F este probabil cea mai frecventă.

Observând acest lucru, criptanalistul ar trage concluzia că F îl înlocuieşte pe E. Apoi, el ar putea observa faptul că UIF apare mai des decât orice alt cuvânt format din trei litere, presupunând că îl înlocuieşte pe THE. În acest moment, ar putea ghici şi faptul că fiecare literă în textul cifrat înlocuieşte litera premergătoare din alfabet şi, testând această ipoteză, ar descoperi că este corectă.

După cum se poate vedea din acest exemplu simplu, cantitatea de materie primă pe care o poate obţine criptanalistul este un factor important care poate influenţa identificarea unei soluţii. Într-un mesaj scurt, E nu apare neapărat în mod frecvent: În exemplul nostru (“Atac sâmbăta”) nu apare deloc. Cu toate acestea, într-un mesaj mai lung sau într-o înşiruire de mesaje, se aplică legea probabilităţii. Este puţin probabil ca frecvenţa literelor (sau grupurilor mici de litere) din textul iniţial să difere foarte mult de cea cu care apar în textele obişnuite în limba engleză. [1]

Istoria criptologiei este fascinantă, dar textul de faţă nu ne permite să intrăm în detalii.[2] În scopul lucrării de faţă, vom identifica trei perioade, în funcţie de tehnologia existentă pentru criptarea mesajelor.

În prima perioadă, începând din antichitate şi până în anii 1930, mesajele erau criptate manual. Existau diverse tehnici, liste de coduri, cifruri de transpoziţie şi de substituţie. La sfârşitul acestei perioade listele de coduri cuprindeau mii de articole. Totuşi, din moment ce acestea erau folosite perioade îndelungate, criptanaliştii le puteau reconstitui. În mod similar, pentru obţinerea unui text cifrat, trebuia efectuate manual o serie de modificări, ceea ce a redus complexitatea cifrurilor şi a uşurat munca criptanaliştilor. Cu cât algoritmul de criptare devine mai complex, creşte posibilitatea apariţiei unei erori de criptare sau decriptare, de aceea cifrurile mai greu de “spart” nu sunt întotdeauna practice.

Bineînţeles că cea mai uşoară metodă de spargere a unui cod este de a fura sau de a obţine prin orice alt mijloc o copie a listei de coduri. Din moment ce crearea unei liste de coduri şi distribuirea ei este un lucru dificil, codurile erau utilizate o perioadă îndelungată, ceea ce sporea utilitatea listei de coduri.

Atât înaintea Primului Război Mondial cât şi în timpul acestuia, marile puteri ale Europei deţineau birouri speciale unde se decriptau mesajele militare şi diplomatice străine. De exemplu, la începutul Primului

Război Mondial englezii au obținã (de pe navele capturate sau scufundate) copii ale principalelor liste de coduri maritime germane. Germanii au luat măsuri suplimentare de siguranță, criptând mesajele deja codate, cu toate acestea, britanicii au reuşit să le descifreze.[3]

Totuşi, cel mai important succes criptanalitic englez l-a reprezentat descifrarea codurilor folosite de diplomația germană. La data de 17 ianuarie 1917, criptanaliştii britanici au descifrat un mesaj, cunoscut în istorie drept "telegrama Zimmermann", prin care ministrul de externe german i-a transmis instrucțiuni ambasadorului german din Mexic cu privire la o posibilă alianță germano-mexicană împotriva Statelor Unite, în cazul în care americanii ar fi răspuns la atacurile germane submarine, (programat pentru 1 februarie), declarând război Germaniei. Decizia Preşedintelui american Woodrow Wilson de a declara război a fost influențată decisiv de publicarea în ziarele din SUA a telegramei din care se deducea că Mexicul intenționează să recupereze Texas-ul, New Mexico şi Arizona. Iscusința cu care a fost publicată telegrama nu a dat de bănuit părții germane că ar fi fost posibilă spargerea codului utilizat.[4]

Spre deosebire de europeni, la începutul Primului Război Mondial americanii nu aveau încă experiență în domeniul criptografiei. Istoria criptografiei americane din timpul războiului şi din următorii zece ani arată cum, în ciuda provocărilor intelectuale deosebite, încă era posibil ca un specialist, lucrând pe cont propriu sau cu un grup restrâns de colaboratori, să descopere principiile fundamentale ale criptării şi să descopere coduri şi cifruri folosite pentru criptarea celor mai importante mesaje. Herbert Yardley povesteşte cum, lucrând de unul singur, a reuşit să criptanalizeze un mesaj trimis preşedintelui Wilson de colonelul Edward House, delegatul personal al lui Wilson, aflat în momentul respectiv în misiune diplomatică în Germania.[5] Relatarea lui Yardley despre perioada în care s-a aflat la conducerea departamentului de criptanaliză a armatei Statelor Unite, în momentul intrării acesteia în război, precum şi a "Black Chamber" din cadrul Departamentului de Stat după încheierea războiului, indică faptul că la acel moment criptografia era mai degrabă o artă decât o ştiință şi în ce măsură perspicacitatea şi intuiția specialiştilor a influențat acest domeniu.

Totuşi, în criptologie, ca şi în alte domenii ale activităților militare şi de informații, Primul Război Mondial a reprezentat o etapă esențială. Conform unui istoric,

> Primul Război Mondial a marcat punctul de cotitură în istoria criptologiei. Înainte de război, domeniul era unul restrâns; după încheierea războiului, acesta a luat amploare. Războiul a marcat dezvoltarea acestei ştiințe. Principalul motor al acestei evoluții a fost creşterea semnificativă a nivelului de comunicații radio. [6]

Spargerea unui cod sau cifru utilizat de inamic reprezenta un avantaj semnificativ în condițiile creşterii traficului radio. În acelaşi timp, un trafic

mai mare sporea vulnerabilitatea codurilor şi cifrurilor de o complexitate similară față de metodele de criptanaliză; deoarece existând mai multe mesaje (criptate cu acelaşi cod sau cifru), criptanalistul avea mai multe şanse să identifice tiparele repetitive care permit găsirea unei soluții.

Traficul radio sporit ducea la supraîncărcarea sistemului manual de criptare şi decriptarea. Acest lucru, coroborat cu necesitatea unor sisteme de criptare mai sigure, a reprezentat cea de-a doua perioadă din istoria acestei ştiințe, în care aparatele mecanice şi electromecanice, cum ar fi maşina de criptare americană Hagelin, Enigma germană şi maşinile japoneze "Purple" (Maşina de scris alfabetică 97) au fost folosite pentru a cripta texte.

Astfel de maşini puteau utiliza algoritmi şi formule mult mai complicate decât cele folosite în perioada în care criptarea se realiza manual. Prin urmare, tehnicile şi procedurile criptanalitice atingeau un nivel de complexitate similar. Spargerea codurilor a necesitat crearea şi utilizarea primelor maşini de calcul şi a determinat progrese în statistică şi în alte ramuri ale matematicii teoretice.[7] În timpul celui de-al Doilea Război Mondial, s-a scris un număr impresionant de articole despre maşinile electromecanice de criptare, cum ar fi Enigma şi "Purple".[8]

Ne aflăm în prezent în cea de-a treia perioadă din istoria acestei ştiințe care este caracterizată de utilizarea computerelor pentru criptarea şi decriptarea mesajelor şi în sprijinul eforturilor criptanalitice. În mod evident, acesta este un subiect foarte sensibil despre care publicul nu are foarte multe informații. Dezvoltarea "criptografiei publice" – studierea şi folosirea criptografiei de către oameni de ştiință sau oameni de afaceri independenți – a furnizat publicului un volum mare de informații despre acest domeniu.[9] Totuşi, nu este posibil să comparăm metodele criptografiei publice cu cea a agențiilor de informații, bazându-ne doar pe surse nesecrete.

Cu toate acestea, poate fi prezentată situația actuală şi punctele forte ale anumitor țări în domeniul criptologiei. Dat fiind rolul computerelor şi monopolul deținut de SUA în domeniul IT, concluzia ar fi că americanii au un avantaj în procesul de decriptare; într-o anumită măsură, această influență poate fi contracarată de progresele altor state (de exemplu ale Rusiei) în domeniul matematicii teoretice.

În acelaşi timp, s-ar părea că progresele în domeniul IT (în ceea ce priveşte viteza cu care se efectuează operațiile aritmetice de bază) favorizează domeniul apărării. Cu alte cuvinte, deşi progresul în domeniul IT permite atât celui care criptează să folosească cifruri cu un grad mai ridicat de complexitate, cât şi criptanalistului să le soluționeze, avantajul este de partea celui care realizează criptările. Progresul în domeniul IT permite obținerea unor cifruri mai complexe pe care aceleaşi computere nu le pot sparge. Dacă aceasta este situația, pe termen lung, criptanaliştii nu au şanse foarte mari de a sparge cifrurile marilor puteri utilizând cea mai avansată tehnologie în domeniu. În practică, desigur, dacă din cauza unei erori în configurare nu este utilizată pe deplin tehnologia computațională existentă în realizarea unui cifru, acesta va fi mai vulnerabil. În plus, criptanaliştii pot profita de utilizarea greşită a unui cifru pentru a-l sparge.[10] Agenții pot

furniza listele de coduri ale inamicului, algoritmi de criptare, astfel permițând unei serviciu de informații să decripteze mesaje ale căror sisteme de criptare nu au putut fi sparte prin criptanaliză.[11]

Vulnerabilitatea criptanalizei. Criptanaliza este una dintre cele mai fragile metode de informații, deoarece țările pot schimba sistemul de criptare în momentul în care își dă seama că inamicul îi poate descifra mesajele. Astfel, nu este surprinzător faptul că succesele criptanalitice americane şi engleze din timpul celui de-al Doilea Război Mondial s-au numărat printre cele mai importante secrete de război, beneficiind de cel mai înalt nivel de securitate. Englezii au ținut secret timp de 30 de ani faptul că au descoperit modul de funcționare al maşinii de criptat germane Enigma, în ciuda numărului mare de oameni implicați în operațiune.

Experiența americană a fost foarte diferită. Publicarea la data de 7 iunie 1942, a unui articol de către *Chicago Tribune* despre victoria SUA în Bătălia de la Midway a reprezentat una din cele mai grave breşe de securitate din timpul războiului. Intitulat "Forțele navale au aflat de un posibil atac japonez", articolul cita materiale rezultate din mesajele japoneze decodate. Acestea au cuprins nu doar numele transportoarelor japoneze implicate, ci şi a crucişătoarelor care sprijiniseră viitoarele forțele de ocupație. În plus, articolul susținea că atunci când flota japoneză a înaintat spre Midway, "toate avanposturile americane au fost avertizate" şi că serviciile de informații ale marinei americane au anticipat "un atac simulat la o bază americană [Dutch Harbor, în insulele Aleutine], care avea să fie însoțit de încercări importante de invadare şi ocupare a unei alte baze militare [Insula Midway]."[12]

Un expert japonez în informații ar fi concluzionat în urma articolului că Statele Unite au avut acces la mesajele japoneze codificate privind acțiunile maritime. Problema a fost prezentată în fața juraților Curții din Chicago; totuşi, nici unul dintre inculpați nu a fost pus sub acuzare. Se pare că înalți funcționari ai administrației americane s-au pronunțat împotriva urmăririi în justiție a inculpaților, pe motivul că un proces ar atrage atenția asupra articolului şi ar fi fost necesară o confirmare publică a faptului că SUA citea mesaje japoneze codate privind acțiunile maritime. (În mod ironic, la data de 31 august 1942 un congresman a menționat acest lucru într-un discurs criticând aspru felul în care ziarul *Tribune* "s-a folosit în mod greşit şi nechibzuit de libertatea presei.")[13]

Juriul încă nu s-a exprimat dacă japonezii au beneficiat sau nu de pe urma acestei "scurgeri" de informații. Este adevărat că la data de 14 august 1942 marina japoneză a introdus o nouă versiune a codului (numit de către criptanaliştii americani JN-25d). Apariția unei noi versiuni a codului la atât de scurt timp după introducerea (la 1 iunie) versiunii anterioare (JN-25c) ridica suspiciuni.[14] Totuşi, noua versiune a codului "păstra caracteristicile formulei extinse JN-25", permițând astfel Statelor Unite să obțină din nou acces la mesajele japoneze mult mai uşor decât dacă japonezii ar fi introdus un sistem cu totul nou.[15] Cu toate acestea, Statelor Unite le-a luat patru luni

pentru a cunoaşte codul JN-25d la fel de bine precum cunoşteau versiunea anterioară.[16]

Un exemplu mai clar de vulnerabilitate a criptanalizei, care priveşte de data aceasta Marea Britanie, a avut loc în anul 1927. În anii precedenţi, biroul criptanalitic englez, Şcoala pentru coduri şi cifruri guvernamentale a reuşit să decripteze mesajele transmise între sediul Comintern (Internaţionala Comunistă) şi guvernul sovietic din Moscova, pe de o parte, şi diferiţi reprezentanţi sovietici la Londra – ambasada rusă, precum şi o comisie comercială şi un birou comercial al Arcos, Societatea Cooperatistă Rusă – pe de altă parte. Astfel, guvernul englez a urmărit activitatea diplomaţilor ruşi şi a delegaţilor comerciali, care includea spionajul şi implicarea în activitatea sindicatelor engleze. În anul 1927, englezii au invocat încălcarea uzanţelor diplomatice întrerupând legăturile cu Uniunea Sovietică. Datorită faptului că în Parlament s-a solicitat argumentarea acestei decizii, miniştrii englezi au dezvăluit public faptul că aveau capacitatea de a decripta mesajele sovietice. După cum era de aşteptat, Uniunea Sovietică a introdus noi cifruri, pe care englezii nu au reuşit să le spargă.[17]

Un caz asemănător, în care un guvern ales în mod democratic, a dezvăluit tipul de capacităţi criptanalitice deţinute pentru a obţine sprijinul pentru politicile sale, dar a pierdut în acelaşi timp posibilitatea de decriptare a mesajelor, se pare că a avut loc în Statele Unite în anul 1986. Pentru a justifica eventuala decizie de a bombarda facilităţile guvernamentale din Tripoli, Libia,

> Preşedintele [Ronald] Reagan [conform *Washington Post*] şi cei mai importanţi consilieri ai săi au făcut o extraordinară dezvăluire privind informaţiile sensibile… pentru a demonstra că Statele Unite aveau dovada că Libia… era direct responsabilă pentru bombardarea unui bar de noapte din Berlinul de vest…
>
> Detaliile prezentate de preşedinte[,] … relatează sursele, vor evidenţia faptul că Statele Unite pot intercepta şi decodifica comunicaţiile diplomatice ale Libiei.[18]

După cum era de aşteptat: "Dezvăluirea publică a capacităţii de decodare a comunicaţiilor diplomatice libiene a dus la pierderea unei surse de informaţii valoroase pentru analiştii de informaţii americani, a cărei înlocuire va dura săptămâni sau chiar luni de zile, au declarat astăzi oficiali din Administraţie."[19]

Aceste exemple vin în sprijinul unei teorii generale despre informaţiile secrete care se poate aplica şi în cazul altor tehnici de analiză şi culegere: cu cât sunt mai valoroase informaţiile existente, cu atât eşti mai reticent în utilizarea lor şi probabil acest lucru atrage atenţia inamicului asupra capacităţilor de culegere de informaţii. În cazul unui guvern democratic, dilemă este cu atât mai dificilă cu cât acesta se vede nevoit să dezvăluie informaţii despre metodele sale de culegere de informaţii pentru a

convinge opinia publică de faptul că strategia sa de guvernare este fundamentată. Dar orice guvernare se confruntă într-un fel sau altul cu această dilemă, atunci când deține informații secrete pe baza cărora intenționează să acționeze.

Cel mai probabil, această problemă poate apărea în timp de război, când impulsul de a acționa pe baza acestor informații este foarte puternic. De exemplu, în timpul celui de-al Doilea Război Mondial englezii ştiau, din interceptarea şi decriptarea comunicațiilor, programul exact al navelor germane care transportau provizii pe Mediterană, pentru forțele generalului Erwin Rommel aflate în Africa de Nord. Cu toate acestea, pentru a nu trezi suspiciuni germanilor în privința securității comunicațiilor, englezii acționau conform regulii care prevedeau că nicio navă nu poate fi atacată înainte de a fi survolată de aeronavele de recunoaştere, astfel acordându-le germanilor o explicație despre modul în care englezii au reuşit să le identifice navele.

Acest punct de vedere este ilustrat şi de faptul că, din câte se pare, primul ministru britanic Winston Churchill aflase de raidul aerian german nimicitor asupra oraşului englez Coventry înainte ca acesta să se producă, dar nu a luat nici o măsură pentru a avertiza apărarea antiaeriană sau serviciile de urgență, de teamă să nu compromită capacitățile britanice de decriptare a mesajelor Luftwaffe. Cercetărilor istorice au infirmat această ipoteză: informațiile culese prin interceptarea comunicațiilor nu au permis englezilor să identifice Coventry drept ținta atacului.[20] Totuşi, povestea oferă o descriere destul de dramatică a dilemelor morale şi strategice cu care un guvern *s-ar putea* confrunta pentru a decide dacă ar trebui să rişte o sursă de informații folosind informațiile oferite de aceasta.

Analiza telemetrică. Telemetria reprezintă transmisia radio de informații de la un vehicul test către o stație de la sol – informații privind funcționarea vehiculului (de exemplu, accelerația sau forța de propulsie a motorului), starea acestuia (cum ar fi temperatura diferitelor componente sau numărul de vibrații înregistrat) sau alte caracteristici. Scopul constă în furnizarea datelor necesare inginerilor care efectuează testul, pentru a evalua performanța vehiculului sau, în caz de eşec, pentru a determina cauza acestuia. Pe baza acestor informații, inginerii reconstituie profilul de zbor la vehiculului şi se asigură de siguranța acestuia, ori fac alte modificări necesare.

Totuşi, aceleaşi semnale radio pot fi interceptate de către un serviciu de informații străin printr-o metodă de culegere numită informații din telemetrie, ori *telint.* Analiza telemetrică este procesul prin care datele telint sunt folosite pentru a deduce caracteristicile de bază ale unui vehicul test. Desigur, în momentul în care inginerii care efectuează testul interpretează datele, ştiu deja, din structura sistemului telemetric, la care dintre caracteristicile rachetei se referă fiecare parte din fluxul de sistem (sau "canalul" telemetric). Pe de altă parte, analiştii de date din telemetrie aflați în slujba unui serviciu străin, nu dețin astfel de informații la început; trebuie să stabilească pe baza informațiilor radio care este caracteristica măsurată de

fiecare canal.[21] Odată ce au fost stabilite aceste aspecte, analiştii pot încerca să creeze un model de rachetă pe computer, de unde pot deriva caracteristici cum ar fi greutatea iniţială (greutatea de lansare) şi încărcătura utilă (focosul "greutatea de aruncare").

Pentru a fi la curent cu ultimele noutăţi privind programele de armament strategic ale Uniunii Sovietice şi a monitoriza respectarea de către Moscova a acordurilor de control al armamentului s-a utilizat analiza telemetrică. Totuşi, asemeni criptanalizei, analiza telemetrică prezintă vulnerabilităţi. În momentul în care un guvern înţelege cât de importante sunt informaţiile telemetrice privind programul de înarmare a unui inamic şi identifică modalitatea în care ar putea fi culese datele telemetrice privind propriul program, acesta poate lua măsuri pentru prevenirea scurgerii acestor informaţii. De exemplu, în timpul dezbaterilor de ratificare a SALT II în anul 1979, a devenit clar faptul că Statele Unite s-au bazat în principal pe datele telemetrice obţinute de la sovietici pentru a monitoriza programul de înarmare cu rachete şi pentru a verifica în ce măsură ruşii respectau acordul. În plus, până la sfârşitul anilor 1970, serviciile de informaţii sovietice ajunseseră prin intermediul spionajului la o cunoaştere detaliată a modalităţii în care Statele Unite culegeau din spaţiu date telemetrice privind rachetele sovietice. Indiferent de motive, din acel moment, Uniunea Sovietică a codificat informaţiile obţinute prin telemetrie în urma testelor cu rachete, împiedicând accesul serviciilor secrete SUA la aceste informaţii.[22]

Nu se ştie în ce măsură este posibilă criptanaliza datelor codificate din telemetrie. Există şi alte metode în afară de criptare pentru a bloca accesul serviciilor de informaţii adverse la informaţiile din telemetrie. După cum am arătat în capitolul precedent, datele pot fi stocate pe o bandă în interiorul unei capsule cu înveliş de protecţie (asemănătoare "cutiei negre" instalate pe aeronavele comerciale) care nu este distrusă în contact cu atmosfera şi în momentul impactului cu solul şi care poate fi recuperată de la bordul vehiculului. În mod similar, datele telemetrice dintr-o rachetă de croazieră sau un avion experimental pot fi transmise la o tensiune joasă către un avion de "urmărire", care zboară aproape de aceasta şi să fie înregistrate la bord; dacă semnalul radio este destul de slab, acesta poate fi imposibil de interceptat din afara zonei de test.

Interpretarea foto. În ciuda echipamentului sofisticat care poate face fotografii în interiorul unui teritoriu inaccesibil, nu s-a descoperit nici un instrument mai eficient decât ochiul uman pentru studierea fotografiilor. Aceasta nu este o sarcină atât de uşoară pe cât pare; deşi deseori se spune că fotografiile sunt o formă de informaţii secrete foarte convingătoare (în sensul că înalţii oficiali sunt mai siguri de informaţiile primite atunci când "le văd cu ochii lor"), fotografia de supraveghere obişnuită este probabil indescifrabilă pentru un amator. Abia după ce analistul foto (PI) identifică aspectele de interes, acestea vor deveni clare şi pentru cei care nu sunt de specialitate.[23]

Calitatea unui sistem fotografic de recunoaştere este de obicei evaluată în funcţie de ceea ce numim "distanţa de rezoluţie de la sol". Acest termen tehnic defineşte mărimea celui mai mic obiect care poate fi identificat dintr-o mulţime de obiecte sau din fundal. Deşi mulţi alţi factori trebuie luaţi în calcul pentru a determina cât de bine poate fi interpretată o fotografie, distanţa de rezoluţie de la sol este "totuşi … o metodă convenabilă pentru a face o comparaţie şi evaluare aproximativă."[24] Pe măsură ce rezoluţia de la sol creşte, va spori şi cantitatea de informaţii ce pot fi extrase dintr-o fotografie. În general, calitatea unei fotografii este evaluată în funcţie de tipul analizei care se poate aplica respectivei ţinte. De exemplu, poate fi detectat un aparat de zbor (cum ar fi un avion), se poate face o identificare aproximativă (identificarea unui anumit tip de avion), o identificare exactă (stabilirea unei anumite variante a acelui tip de avion) sau (în scopul analizei tehnice) se poate face o descriere detaliată?[25]

Distanţele reale de rezoluţie de la sol pe care le pot obţine sateliţii de supraveghere fotografică ai unui serviciu de informaţii sunt secrete, întrucât aceste informaţii le pot indica inamicilor ce tip de detalii (de echipament militar, facilităţi ş.a.m.d.) pot vedea sau nu serviciile. Astfel de informaţii sunt utile oricărui strateg militar care doreşte să păstreze secrete anumite detalii ale noilor sisteme de armament. Aceste informaţii s-ar dovedi utile şi în cazul specialiştilor care elaborează strategiile de dezinformare, deoarece le-ar putea indica în ce măsură ar fi posibilă diferenţierea dintre un obiect real şi unul fals prin procedurile de supraveghere fotografică.

Oricât ar fi de bună rezoluţia, dintr-o fotografie nu pot fi extrase direct toate tipurile de informaţii. Analiştii fotografici trebuie să lucreze pe baza a ceea ce numim "semnături" – detalii specifice care, în funcţie de experienţă sau logică, sunt asociate cu anumite echipamente, activităţi, intenţia de a lua măsuri în viitor şi aşa mai departe.[26] De exemplu, extinderea pistei unui aerodrom ar fi necesară în cazul aterizării unui nou tip de aeronavă; bazându-se pe experienţă, un analist ştie că lungimea pistei este corelată cu prezenţa unui anumit tip de aeronavă şi ar putea concluziona că o astfel de aeronavă va staţiona pe acel aerodrom. În mod asemănător, analiştii au ajuns la concluzia că diferenţa dintre o bază militară sovietică şi una cubaneză constă în forma de teren de fotbal a uneia faţă de forma de teren de baseball a celeilalte.

Una dintre metodele de utilizare a semnăturilor pe care s-au bazat Statele Unite se numeşte "crateologie" – corelarea echipamentului militar cu tipul şi mărimea avioanelor care sunt folosite la transport. O dată determinat faptul că un anumit avion sau o anumită rachetă a fost transportată în avioane de o anumită mărime, conform principiilor crateologiei, se sugerează că şi alte cutii de aceeaşi mărime ale căror conţinut nu a fost monitorizat direct pot conţine acelaşi tip de avioane sau rachete.[27]

Utilitatea semnăturilor derivă din tendinţa multor organizaţii – în special cele militare – de a urma o rutină, de a face lucrurile "ca la carte". Astfel, când, în anul 1962 Uniunea Sovietică a decis să poziţioneze rachete balistice cu rază de acţiune medie şi mijlocie (MRBM şi respectiv IRBM)

spre Cuba, aceasta a pregătit apărarea insulei prin amplasarea artileriei antiaeriene de-a lungul coastei cubaneze în formă trapezoidală, pe care experţii militari le-au identificat imediat acelaşi scenariu care se aplică şi în cazul rachetelor sovietice SA-2 (sol-aer). Această descoperire a atras un semnal de alarmă serviciilor de informaţii americane cu privire la faptul că pe insulă "se întâmpla ceva extraordinar". În paralel, informaţiile obţinute în urma monitorizării unei misiuni U-2 care a avut loc ulterior au indicat că în vestul Havanei aveau loc lucrări masive de excavare şi de construcţie. Cu toate că experţii nu au identificat la faţa locului rachete sau echipamentele pentru rachete, era sigur faptul că sovieticii plănuiau să construiască o bază pentru rachete IRBM, pornind de la modelul de construcţie şi excavaţie pe care l-au găsit acolo. Într-adevăr, când unuia dintre experţi "i-au fost arătate fotografiile de la bazele din Cuba, el a arătat un manual de operaţiuni a unei astfel de baze aflate în Rusia [IRBM] în Rusia."[28]

Utilizarea semnăturilor poate fi foarte eficientă, dar poate da naştere şi la multe erori. În timpul crizei rachetelor din Cuba, locaţia focoaselor nucleare ale rachetelor a reprezentat o informaţie definitorie. Fuseseră deja trimise în Cuba, şi dacă da, unde erau? Utilizând semnături rezultate din fotografii ale instalaţiilor nucleare din Uniunea Sovietică, experţii americani au asociat depozitele de armament nuclear cu măsuri de securitate extinse şi elaborate. Întrucât armamentul a fost utilizat pentru prima dată în afara Uniunii Sovietice, era normal ca focoasele să fie controlate cu şi mai mare strictețe. Prin urmare, datorită absenţei oricăror activităţi stricte de monitorizare a bazelor de lansare sau a buncărelor pentru depozitarea armamentului aflate în construcţie, experţii au ajuns la concluzia că focoasele nu luaseră încă drumul Cubei.

Totuşi, în timpul evenimentelor, s-a trecut la o analiză mai amănunţită a fotografiilor care a dezvăluit faptul că focoasele se aflaseră de la bun început acolo, depozitate în camioane aparent inofensive. În lipsa unor elemente care să identifice luarea unor măsuri speciale de securitate a zonei sau a vreunei activităţi în jurul vehiculelor, analiştii nu au semnalizat camioanele sau le-au clasificat în mod generic drept vehicule pentru transportarea diverselor tipuri de rachete. Abia mai târziu aceste camioane au devenit elemente de maximă importanţă, făcându-se legătura cu facilităţile armamentului nuclear sovietic în Rusia şi Europa de Est.[29]

În plus, dacă adversarul identifică semnăturile pe care se bazează experţii, el le poate folosi în avantajul său, inclusiv pentru planuri de diversiune. Conform anumitor relatări, guvernul indian s-a bazat pe astfel de informaţii pentru a ascunde de serviciile secrete americane pregătirile pentru testele sale nucleare din anul 1998. Datele pe care guvernul indian le culesese în legătură cu semnăturile pe care se bazau Statele Unite proveneau în urma analizei unui incident ce a avut loc cu trei ani înainte, moment în care India plănuia să efectueze teste nucleare. Ca măsură diplomatică iniţiată de către Statele Unite în vederea dejucării planurile Indiei, administraţia americană a explicat care au fost motivele îngrijorării referitoare la iminenţa efectuării unor teste nucleare; în cadrul acestui demers, specialiştii americani

le-au arătat oficialilor indieni fotografii captate din satelit care arătau indicatorii specifici (semnături) unui test nuclear iminent. Astfel, s-a dovedit faptul că în anul 1998, guvernul indian avea mai multă experienţă în a masca pregătirile pentru un test nuclear (de exemplu, îngropând cablurile care făceau legătura dintre centrul de control şi amplasamentul de testare).[30]

Bănci de date (cercetare de bază)

După cum am prezentat deja la secţiunea culegerii informaţiilor din surse deschise, o funcţie importantă şi frecventă a serviciilor de informaţii este asamblarea şi întreţinerea bazelor mari de date, care acoperă probleme importante pentru politica militată şi externă a guvernului. Această activitate poate consta în realizarea de baze de date cu informaţii relevante despre toate ţările unde ar putea avea loc o activitate militară.[31] Astfel de compendii au scopul de a deveni un instrument de lucru pentru strategii militari, care privesc ţara ca pe o posibilă zonă de luptă, şi care conţin informaţii detaliate despre forţe militare existente, facilităţi militare şi de transport, topografie militară, precum şi informaţii despre politica, demografia, industria şi agricultura ţării.

Deşi problemele analitice care apar atunci când se realizează o astfel de bază de date sunt minime, este necesar să se ştie care informaţii sunt importante şi care nu. Deciziile cu privire la ţările care urmează a reprezenta un viitor teatru de operaţiuni precum şi gradul de dificultate pe care îl implică aceste activităţi au consecinţe foarte importante în cazul în care informaţiile cuprinse în compendiu vor fi susţinute de către operaţiuni militare. De exemplu, planul prin care Statele Unite şi ţările Organizaţiei Statelor Caraibilor de Est urmau să invadeze Granada a avut un ritm foarte rapid de evoluţie. O consecinţă negativă a fost faptul că nu erau disponibile hărţi militare adecvate. Conform celor spuse de amiralul Wesley McDonald, comandantul forţelor americane în Atlantic, "Armata, în special trupele terestre, au folosit iniţial hărţile drumurilor sau alte tipuri de hărţi, ceea ce făcea dificilă determinarea … coordonatelor reţelei. Aceasta este una dintre lecţiile pe care le-am învăţat."[32]

Alte tipuri de bănci de date sunt puse la dispoziţia analiştilor de informaţii. De exemplu, după cum am arătat deja, colectarea şi analizarea cantităţilor mari de informaţii nesecrete pot furniza o mai bună cunoaştere a unei societăţi închise, cum sunt fosta Uniune Sovietică, China şi Coreea de Nord. Documente conţinând date biografice (conţinând referinţe din ziare cu privire la partide şi oficiali ai guvernului, poziţiile lor, promovări, călătorii şi aşa mai departe), de exemplu, pot fi analizate pentru a clarifica relaţiile acestora cu oficiali, lupte interne în cadrul partidelor şi alte aspecte de acest gen.

Elaborarea informaţiilor finite

Tipurile de analiză pe care le-am descris mai sus reprezintă paşii iniţiali necesari în procesul analitic; în cea mai mare parte, rezultatele acestei

munci servesc drept sursă pentru alți analiști de informații, dar nu ajung direct la factorii decizionali sau la comandanți (utilizatorul final de informații). Această secțiune prezintă tipurile de informații finite produse. Aceste tehnici folosite nu sunt nici atât de rigide ca și criptanaliza sau analiza telemetrică și nici la fel de originale ca activitatea de culegere de informații. În unele cazuri, cum ar fi elaborarea de informații economice și politice, tehnicile nu pot fi distinse de acelea corespunzătoare științelor sociale.

Informații științifice și tehnice. În timpul și în perioada imediat următoare celui de-al II-lea Război Mondial, a crescut gradual ritmul în care au fost asimilate noile principii științifice și tehnice destinate domeniului militar. Capacitatea militară a unei națiuni s-a fundamentat pe dezvoltarea tehnologică și pe capacitatea de producție a sistemelor militare care încorporau acea tehnologie, pe capacitatea generală de producție, pe dimensiunea forței sale militare și pe orice alt element de referință în domeniul militar. Acest lucru era valabil în mod special în cazul unui război aerian, domeniu care a cunoscut introducerea radarului aerian, a sistemelor de navigație sofisticate pentru ghidarea bombardierelor către țintele lor, a avioanelor cu reacție, a rachetelor balistice și de croazieră, și, în final, a bombei atomice. Astfel, culegerea informațiilor cu privire la sistemul militar deținut de inamic a devenit un obiectiv important pentru agențiile de securitate ale fiecărei țări. A devenit important să se obțină informații detaliate despre modul de funcționare a unui sistem în vederea identificării metodelor de contracarare.

Acest lucru a impus o nouă sarcină serviciilor de informații, și anume prezicerea apariției noilor tehnologii și cunoașterea modului lor de funcționare în vederea contracarării acestora.[33] Prin urmare, agențiile de informații au solicitat să aibă acces la informații științifice și tehnice specializate și ca această capacitate să fie integrată în procesul informatic.

Activitatea de culegere de informații din domeniul tehnic și științific trebuie să fie mai detaliată decât orice altă activitate de culegere de informații pentru ca un cititor neavizat să știe unde să caute aceste informații. Aceasta înseamnă că este nevoie de o coordonare strânsă între analiști și ofițerii de teren. Procesul trebuie să fie similar metodei științifice în care ipotezele (formulate de către analist) sunt demonstrate mai degrabă prin observații directe decât prin experiment. De exemplu, R.V. Jones, șeful departamentului de informații al Ministerului Aviației din Marea Britanie din timpul celui de-al Doilea Război Mondial, povestește cum teoria sa, privind natura primului sistem de semnale radio (*Knickebein*) folosit de către germani ca ajutor instrument de navigație pentru bombardiere, a fost demonstrată în momentul în care un avion echipat cu receptoare speciale, care zbura într-o anumită zonă desemnată de el, a recepționat semnalele radio pe care a prezis că le va capta în acea zonă.[34]

Analiza în domeniul informațiilor științifice și tehnice necesită combinarea informațiilor cu expertiza științifică sau tehnică. Deși principiile științifice sunt prin natura lor universale și cunoscute de către experții din

întreaga lume, felurile în care sunt aplicate pot diferi de la o țară la alta. Astfel, acest tip de analiză necesită un grad înalt de cunoaştere ale progreselor tehnice şi ştiinţifice în vederea identificării modului de acţiune al inamicului, combinat cu destulă imaginaţie pentru a realiza că inamicul poate soluționa probleme tehnice pe care propria țară a analistului nu a reuşit să o rezolve, sau chiar să ajungă la o soluție diferită, dar totuşi validă.

Informații militare. Informațiile militare sunt acele informații referitoare la bazele militare străine şi sunt folosite în scopul planificării operațiunilor militare ale unei țări în timp de pare sau a derulării operațiunilor militare ale unei țări în timp de război. Cea mai elementară informație militară este cea pe care o numim "ordin de luptă", o înşiruire a informațiilor primare despre forțele militare ale unei țări - numărul de soldați şi a tipurilor de arme, structura organizațională şi date asemănătoare. Caracterizarea acestei informații drept elementară nu înseamnă că este uşor de obținut sau că este un lucru simplu să ştii care este numărul trupelor auxiliare sau a rezerviştilor. Revizuirea ordinului de luptă nord-coreean de către serviciile de informații americane la sfârşitul anilor 1970 este un astfel de caz; peste un an, estimările informative ale numărului trupelor terestre nord-coreene s-au mărit cu o treime. Ajustări similare au fost făcute la numărul de tancuri, lansatoare de rachete şi "tuburi" de artilerie.

O completare necesară la ordinul de luptă ar putea fi reprezentat de informații cu privire la aspectele calitative ale unui amplasament militar străin: calitatea instruirii, calitatea actului de comandă şi alte aspecte asemănătoare.

Mult mai importante decât aceste informații fundamentale sunt cele referitoare la metodele de luptă ale forțelor armate: tactica pentru care au fost instruiți şi pe care au adoptat-o, sub ce formă se va manifesta războiul plănuit şi care va fi strategia pe care o vor adopta. Datele primare pentru aceste informații pot proveni din surse deschise (cum ar fi publicațiile militare), informațiile furnizate în cadrul contactelor stabilite de ataşați sau diplomați cu militari reprezentanți ai statelor considerate adversare, supravegherea (fie directă, fie prin intermediul mijloacelor tehnice secrete) desfăşurărilor de forțe sau ale exercițiilor militare, ori surse umane de informații cu acces direct la planuri militare. În ceea ce priveşte informațiile ştiinţifice şi tehnice, această categorie de analiză necesită combinația dintre prognoza informativă (în care se concentrează toate informațiile despre adversar şi care ilustrează concepția militară a acestuia) şi prognoza analizată de specialiştii militari (care concentrează descrierea capacității militare şi forma în care se va manifesta războiul prognozat).

Specialiştii militari trebuie să dea dovadă de flexibilitate în gândire atunci când emit aceste prognoze în scopul depistării soluțiilor diferite pe care adversarul le-ar putea adopta în cazul problemelor militare obişnuite, soluții care derivă din resursele pe care le dețin aceştia. Pe scurt, "strategii au nevoie de informații referitoare la *diversitatea tipologiilor militare* – informații care să dezvăluie metodele de operare ale inamicului, conflictele

interne şi modul în care acţionează, precum şi aspectele conceptuale divergente."[35]

Un exemplu în acest sens este oferit de către francezi referitor la planurile de luptă germane de la începutul Primului Război Mondial. Strategia germană (Planul Schlieffen) era de a evita un atac direct împotriva Franţei, prin desfăşurarea unor operaţiuni militare în Belgia care au fost urmate de desfăşurări de trupe de-a lungul graniţei franco-belgiene. Totuşi, pentru a pune în aplicare acest plan, a fost nevoie ca germanii să arunce rezerviştii în luptele din linia întâi; în caz contrar, nu ar fi avut destui oameni pentru teatrul de operaţiuni care se desfăşura pe flancul belgian şi pentru poziţiile defensive de-a lungul graniţei franco-germane. Comandanţii francezi deţineau informaţii cu privire la planurile Germaniei pe care le-au subestimat considerând a fi nerealiste: aceştia au refuzat să creadă că omologii lor germani ar trimite în linia întâi rezerviştii din moment ce ei înşişi nu ar fi făcut acest lucru. Astfel, francezii au interpretat greşit locul unde vor ataca germanii – nu din cauza lipsei informaţiilor, ci fiindcă ei nu au putut să înţeleagă faptul că armata germană ar putea opera altfel decât ei.[36]

În cele din urmă, când operaţiunile militare sunt iminente sau chiar încep să se desfăşoare, trebuie să existe informaţii cu privire la dispozitivele militare şi la mişcarea forţelor. Acest tip de informaţii reprezintă datele primare pentru ceea ce cunoaştem sub numele "indicaţii şi avertizări", care se referă la evitarea surprizelor strategice.

Informaţii politice. Informaţiile politice sunt informaţii care privesc procesele politice, idei şi intenţii ale ţărilor străine, factiuni şi lideri. Analiza acestor informaţii este similară cu analiza informaţiilor provenite din surse academice şi jurnalistice precum şi din comentariile cu privire la politica internă şi internaţională a altor state. O diferenţă evidentă constă în existenţa surselor secrete, umane sau tehnice (în principal informaţiile din comunicaţii), care furnizează informaţii ce nu sunt disponibile comentatorului public.

Importanţa acestor surse suplimentare depinde de natura regimului ţării studiate şi de numărul şi calitatea surselor de informaţii despre acea ţară. Cu cât o ţară este mai democrată şi deschisă, cu atât este mai uşor de studiat viaţa sa politică, fără a face apel la sursele de informaţii. În mod contrar, în ţările în care deciziile politice esenţiale sunt luate de către indivizi (ori familii, ori partide), sursele de informaţii devin mai importante şi mai greu de obţinut. Totuşi, chiar şi în cazul unei societăţi închise, pot exista informaţii din surse deschise care, dacă sunt analizate cum trebuie, pot dezvălui mult mai multe lucruri despre viaţa politică decât la primă lectură. De exemplu, după cum am discutat la culegerea de informaţii din surse deschise, informaţiile biografice (cum ar fi faptul că A pare să fie recunoscător lui B pentru promovările sale anterioare) despre liderii unei ţări pot fi analizate pentru a avea o imagine despre luptele interne; chiar şi într-un regim care afişează public o imagine de unitate se pot înţelege luptele interne prin observarea modului în care protejaţii liderului şi-au obţinut poziţia.

În plus față de problema disponibilității unor surse de informații secrete, o diferență importantă între analiza informațiilor provenite din sfera politică şi activitatea academică sau jurnalistică consistă în modul de lucru. Analiştii informatici trebuie să ofere răspunsuri oportune. Munca lor este inutilă dacă nu ajunge la factorii decizionali înainte ca aceştia să fie forțați de circumstanțe să acționeze. Spre deosebire, autorii academici au timpul de partea lor. În plus, cercetătorii desfăşoară o activitate solitară, alegându-şi singuri temele; ofițerii de analiză răspund unor comenzi de informații şi lucrează în echipă.

Conținutul analizelor efectuate de ofițeri analişti în comparație cu cercetătorii sunt determinate de scopul şi de modul în care se desfăşoară aceste activități. Ofițerii de analiză urmăresc să scoată în evidență acele aspecte care interesează factorul politic; cercetătorii urmăresc în mod special doar acele aspecte pe care ei le consideră a fi cele mai importante. Acest aspect este discutat pe larg în capitolul 6, referitor la relația dintre informații şi politică.

Informații economice şi sociale. Informațiile economice şi sociale se referă la aceleaşi fenomene care fac obiectul de activitate al ştiințelor sociale cel puțin în aceeaşi măsură în care acestea interferează cu problemele cotidiene importante. Informațiile politice se concentrează pe acele informațiile cerute de factorii politici. Activitatea de analiză a acestor informații este de multe ori socotită a fi mai puțin complexă – atât în teorie cât şi în practică – față de studiile academice în ciuda faptului că nu apar diferențe substanțiale în modul de lucru.

Nu numai că metodele cercetării academice şi a celor efectuate de specialiştii militari sunt în mare măsură aceleaşi, dar şi specialiştii care lucrează în aceste domenii sunt puşi în fața aceloraşi probleme atunci când efectuează evaluări ale acestor informații, din moment ce foarte puține din acestea sunt obținute prin metode secrete. Aşadar, o estimare efectuată de către un analist de informații cu privire la viitorul unei țări nu va diferi prea mult de estimarea unui cercetător sau de un grup de experți într-o universitate. Cu toate acestea, uneori este nevoie să se aplice metodele de obținere a informațiilor secrete. Multe informații economice despre fosta Uniune Sovietică au fost ținute secret; printre acestea şi informațiile referitoare la rezervele de aur precum şi la anuale de aur pe piața internațională. În timp ce un ofițer de informații sunt deseori forțați să estimeze aceste cifre în acelaşi fel în care ar face-o un economist, o sursă de informații poate furniza indicii sau chiar cifrele oficiale sovietice. Totuşi, contribuția surselor de informații la analiza economică şi socială este redusă.

Agențiile de informații nu pot să atragă cei mai buni analişti în domeniu. Libertatea vieții academice se dovedeşte a fi mai atractivă pentru specialiştii talentați în ştiințe sociale, chiar dacă salariile sunt mai mici. În plus, companiile multinaționale, băncile şi firmele de brokeraj pot supralicita cu uşurință agențiile de informații în ceea ce privește salariile oferite economiştilor calificați. Nu există niciun argument care să justifice faptul că

analizele efectuate de către analiştii de informaţii în problemele economice, informaţii care nu implică societăţile care ţin secrete bazele lor de date să fie superioare celor făcute de către economiştii din lumea afacerilor.[37] Bineînţeles că analiza economică efectuată în lumea afacerilor este văzută ca informaţie cu drept de autor şi nu este disponibilă factorilor decizionali din guvern, dar măcar o parte din ea ar putea fi, prin intermediul serviciilor de consultanţă sau a buletinelor de afaceri.

PRODUSUL ACTIVITĂŢII DE INFORMAŢII

Produsul activităţii de informaţii este reprezentat de orice mijloc, de la un raport oficial la o scurtă conversaţie, prin care un analist de informaţii transmite informaţii prelucrate factorilor de decizie sau comandanţilor militari care au nevoie de informaţiile respective şi le pot utiliza. În secţiunea de faţă sunt analizate diferitele forme pe care le poate lua produsul activităţii de informaţii şi utilitatea acestora. Clasificarea are un caracter general, iar terminologia este cea utilizată în mod obişnuit de agenţiile de informaţii ale SUA, fără a fi însă una complet standardizată.

În general, produsele activităţii de informaţii sunt împărţite în trei categorii: *informaţii curente*, *informaţii de bază* şi *estimări informative*. Această clasificare corespunde modelului propus de Sherman Kent; într-o terminologie proprie, acesta menţionează "forma reportericească curentă" a informaţiilor, "forma descriptivă de bază" şi "forma speculativ-estimativă", arătând că acestea vizează informaţiile referitoare la prezent, trecut şi, respectiv, viitor.[38] Pentru ilustrarea diferitelor tipuri de produse ale activităţii de informaţii am utilizat, în principal, exemple din SUA, deoarece în cazul acestora am avut la dispoziţie informaţii mai detaliate decât pentru alte ţări. Distincţiile au însă aplicabilitate generală, chiar dacă accentul pus pe diferite produse variază de la un serviciu de informaţii la altul.

Informaţiile curente

Agenţiile de informaţii au diverse produse menite să aducă la cunoştinţa factorilor de decizie noile informaţii de interes deosebit care pot influenţa politicile adoptate. În această privinţă, agenţiile au un rol similar celui îndeplinit de presă. [39] Sfera informaţiilor depinde de interesele naţionale. În mod evident, trebuie stabilite anumite priorităţi, în funcţie de ceea ce este, potrivit lui Kent, "relevant pentru problemele naţionale curente şi alte probleme care se întrevăd."[40] Chiar dacă există un sistem de priorităţi, la acesta trebuie să se adauge evaluările specialiştilor din serviciile de informaţii cu privire la aspectele care prezintă importanţă pentru utilizatori. Aceste evaluări depind, la rândul lor, nu numai de perspicacitatea analiştilor de informaţii, ci şi de intensitatea interacţiunii lor cu factorii de decizie.

În Statele Unite, cel mai cunoscut produs de acest gen este *Informarea zilnică a preşedintelui* (PDB). Aceasta trebuie să includă

"informaţii de cea mai mare importanţă, necesare preşedintelui pentru îndeplinirea responsabilităţilor pe linie de securitate naţională" şi "este transmisă doar preşedintelui, vicepreşedintelui şi unui grup restrâns de oficiali din cadrul executivului, desemnaţi de preşedinte."[41] Potrivit aprecierilor făcute în 1980 de Cord Meyer, un fost oficial CIA,

> Este conceput astfel încât să poată fi citit de preşedinte în zece sau cincisprezece minute, la începutul fiecărei zile de lucru. Nu se doreşte a fi o recapitulare a evenimentelor relatate de mass media în decursul ultimelor 24 de ore, ci o scurtă prezentare a semnificaţiei celor relatate de sursele secrete în legătură cu evoluţiile actuale de pe plan mondial. [42]

Informarea principalilor factori de decizie (SEIB), care a înlocuit un document anterior, numit *"Raportul informativ zilnic"*(NID), este distribuit pe scară mai largă. SEIB este "alcătuită în baza consultărilor cu alte agenţii de informaţii" şi include "informaţii curente esenţiale[,]… prezentate astfel încât să răspundă cerinţelor oficialilor de rang înalt din cadrul guvernului Statelor Unite, cu atribuţii în domeniul asigurării securităţii naţionale."[43]

Din când în când se face auzită opinia potrivit căreia agenţiile de informaţii ale SUA dedică prea mult timp şi efort pentru îndeplinirea acestei atribuţii de "informare curentă", ceea ce le afectează capacitatea de a analiza în profunzime diverse situaţii. De exemplu, într-un raport al unei comisii senatoriale privind departamentul analitic al CIA, Direcţia de informaţii (DI), se făceau următoarele comentarii, sub titlul "Sindromul 'Evenimentelor curente'":

> Sarcina de a realiza rapoarte informative curente – care analizează evenimentele zilnice în vederea unei informări rapide – consumă în prezent prea multe resurse din cadrul DI. Răspunzând cererilor sporite de informaţii de interes imediat venite din partea factorilor de decizie, de abordare pe larg a mai multor subiecte, DI a fost nevoită să recurgă, în mare parte a activităţii sale de cercetare, la o abordare axată pe "evenimentele curente". Analiza aprofundată a problemelor cu importanţă pe termen lung pentru factorii de decizie prezintă mai puţin interes şi s-a alocat un volum mai mic de resurse în acest scop…
>
> Potrivit unor observatori, acest sindrom a avut un impact negativ asupra nivelului calitativ al avertizărilor cu privire la posibile crize şi asupra identificării tendinţelor pe termen lung. Abordarea axată pe "evenimente curente" a condus la problema "analizei incrementale" – tendinţa de concentrare asupra celei mai recente informaţii, fără a lua în calcul, în mod sistematic, ansamblul de informaţii integrate acumulate

în timp. Grăbindu-se să sistematizeze datele zilnice, analiştii au tendinţa de a pierde din vedere factorii şi conexiunile ce stau la baza datelor respective.[44]

Din simplu fapt că această critică a continuat să se facă auzită în decursul anilor se poate trage concluzia că presiunile exercitate în direcţia abordării evenimentelor curente – având la bază dorinţa factorilor de decizie de a fi ţinuţi la curent cu ştirile "fierbinţi" – sunt, în mod inerent, puternice şi vor avea deseori câştig de cauză în faţa dorinţei analiştilor de informaţii de a realiza analize de mai mare profunzime.[45] Cu aceleaşi presiuni se confruntă, probabil, şi agenţiile de informaţii din alte ţări.

Semnale şi avertizări

Una dintre cele mai importante funcţii ale unei agenţii de informaţii este aceea de a avertiza din timp cu privire la eventuale acţiuni militare ostile; în era nucleară, importanţa acestei funcţii este cu atât mai evidentă. De fapt, factorul principal care şi-a pus amprenta asupra întregului sistem de informaţii american postbelic a fost reprezentat probabil de faptul că organizaţiile de informaţii antebelice nu au reuşit să transmită o avertizare în legătură cu atacul japonez de la Pearl Harbor.

Dată fiind importanţa sa (în special în perioada Războiului Rece, când Statele Unite, URSS şi aliaţii lor aveau importante forţe armate şi mii de arme nucleare care puteau fi îndreptate împotriva adversarului) şi întrucât putea fi necesară luarea rapidă a unor decizii, această funcţie a agenţiilor de informaţii a fost sistematizată în măsură mult mai mare decât oricare alta (cel puţin în Statele Unite). Sistemul, cunoscut sub numele de *semnale şi avertizări* (I&W), are la bază analizarea demersurilor inevitabile sau probabile pe care le-ar întreprinde un adversar în vederea pregătirii unui atac armat. Aceste evenimente ipotetice – mobilizarea rezerviştilor, poziţionarea avansată a forţelor militare, schimbarea manierei de comunicare şi aşa mai departe – poartă numele de "indicatori"; atunci când evenimentul se produce şi este observat, este numit "semnal". Analiştii stabilesc gravitatea ameninţării în funcţie de ansamblul semnalelor şi emit avertizări de diferite niveluri.[46]

Oleg Gordievski, un ofiţer KGB care a desfăşurat activităţi de spionaj pentru serviciile britanice de informaţii între anii 1975 şi 1985, a dezvăluit o serie de proceduri I&W utilizate de fosta Uniune Sovietică. Potrivit acestuia, în 1981 Politburo a dispus KGB-ului şi serviciului de informaţii militare (GRU, conform iniţialelor ruseşti) să colaboreze în vederea realizării unui nou sistem de monitorizare la scară mondială, astfel încât să poată fi sesizate indiciile unui posibil atac nuclear occidental. GRU răspundea de monitorizarea indicatorilor strict militari, în timp ce KGB-ul urma să urmărească indiciile luării deciziei politice de lansare a unui atac nuclear. Printre indicatorii pe care trebuia să îi monitorizeze rezidenţa KGB din Marea Britanie se numărau:

- Programul activităților de la Downing Street 10 (reşedința primului ministru), Ministerul Apărării, Ministerul de Externe, Ambasada SUA şi sediile centrale ale serviciilor britanice de informații şi securitate (de exemplu, erau luminile aprinse noaptea?)
- Frecvența cu care se deplasau curierii între aceste instituții
- Venirile şi plecările premierului şi ale altor miniştri importanți (de exemplu, făcea premierul mai multe vizite la Palatul Buckingham decât în mod obişnuit?)
- Existența unor măsuri neobişnuite de apărare civilă, cum ar fi constituirea unor rezerve de alimente sau pregătirea unor bănci de sânge pentru situații excepționale.

Rapoartele de rutină urmau să fie elaborate din două în două săptămâni, dar orice evenimente ieşite din comun urmau să fie raportate imediat. [47]

Un astfel de sistem formalizat, în care indicatorii sunt stabiliți în prealabil şi pot orienta într-o anumită măsură procesul de culegere a informațiilor, garantează faptul că informațiile nu sunt ignorate, ci sunt incluse în procesul de elaborare a politicilor. Acest lucru este însă valabil doar în cazul problemelor de importanță deosebită, cum ar fi o posibilă acțiune militară ostilă. În alte privințe nu există, de regulă, un sistem automat care să garanteze luarea în calcul a informațiilor disponibile în procesul decizional.

După ce CIA-ul a fost considerat în mare măsură răspunzător pentru faptul că nu a existat o avertizare cu privire la revoluția iraniană din 1978 - 1979, s-au avansat propuneri de creare a unui sistem politic de I&W, pentru a avertiza în legătură situațiile de instabilitate politică din alte țări. Aceasta ar presupune stabilirea unor indicatori similari celor utilizați în cazul avertizărilor referitoare la eventuale atacuri militare. Acest lucru este mult mai dificil de realizat în domeniul politic comparativ cu cel militar, aşa cum a demonstrat-o, o dată în plus, prăbuşirea rapidă şi neaşteptată a regimurilor comuniste din Europa de Est, în 1989, şi din Uniunea Sovietică, în 1991; este puțin probabil ca stadiul actual al ştiințelor sociale să permită obținerea unor rezultate suficient de credibile, astfel încât să aibă o utilitate reală. Cu toate acestea, un sistem mai riguros ar clarifica responsabilitățile ce revin agenților de informații în ceea ce priveşte transmiterea de avertizări cu privire la posibile evenimente grave, chiar şi atunci când factorii de decizie nu îşi concentrează atenția asupra respectivei țări sau regiuni.

Informațiile de bază

O altă categorie generală de produse ale activității de informații este "raportul informativ de bază". Un astfel de raport încearcă să ofere o imagine cât mai completă a unei anumite situații, valorificând atât date din surse deschise, cât şi informații relevante obținute din toate sursele secrete

disponibile. De exemplu, în domeniul militar, un produs de acest gen se poate referi la dispozitivul de luptă. În mod asemănător, un raport informativ de bază privind sistemul politic al unei țări poate include o trecere în revistă a tuturor forțelor şi personalităților politice importante, a viziunilor lor tradiționale, a legăturilor dintre ele şi aşa mai departe.

Rapoartele periodice

După cum I&W reprezintă o formă sistematizată a informațiilor curente referitoare la o anumită problemă de mare importanță, pot exista serii speciale de rapoarte care abordează anumite probleme. De exemplu, în perioada Războiului Rece, serviciile americane de informații au realizat rapoarte semestriale referitoare la modul în care sovieticii respectau acordurile privind armele nucleare strategice; aceste rapoarte conțin cele mai solide evaluări în legătură cu forțele nucleare strategice ale țării respective, cu relevanță pentru acordurile în cauză. În 2001, Direcția de Informații a CIA (DI) a prezentat pe website-ul său următoarea listă de rapoarte periodice:

- *Regional Reviews*. Evaluări periodice (începând de la unele cu frecvență zilnică, până la cele lunare) ale problemelor politice, economice, militare şi sociale din alte țări, cu relevanță pentru interesele SUA … care abordează evenimente regionale şi naționale din Africa, Europa, America Latină, Orientul Mijlociu, Asia şi statele slave şi euroasiatice din fosta Uniune Sovietică.
- *The Terrorism Review*. Un raport lunar, care analizează tendințele actuale ale terorismului internațional şi metodele utilizate, … inclusiv o cronologie a incidentelor teroriste care au avut loc pe plan internațional.
- *The Narcotics Monitor*, care analizează evoluțiile înregistrate pe plan mondial în domeniul narcoticelor.
- *Proliferation Digest*, care apare lunar şi cuprinde articole pe teme de proliferare.
- *The International Arms Trade Report*, cu apariție bilunară.

Rapoartele informative cu evoluții de perspectivă

Cea mai ambițioasă categorie de produse ale activității de informații este aceea care nu se limitează la descrierea situației actuale, ci încearcă să anticipeze modul în care va evolua ea. În limbajul serviciilor americane de informații, astfel de lucrări sunt numite estimări. Un loc aparte îl ocupă *estimarea națională de securitate* (NIE), care reprezintă cea mai fundamentată opinie exprimată cu privire la un anumit subiect, de comunitatea agenților americane de informații.

Aceste estimări sunt menite să ofere cea mai amplă viziune asupra subiectului în cauză şi să proiecteze situația actuală în viitor. În Statele

Unite, ele sunt realizate de un personal special desemnat, cu sprijinul analiştilor din toate agenţiile de informaţii. Estimările includ punctele de vedere ale tuturor agenţiilor din cadrul comunităţii de informaţii.[48] Se depun mari eforturi pentru a se ajunge la un consens, dar, atunci când acest lucru nu este posibil, se poate exprima o opinie diferită într-o "notă de subsol", chiar dacă opinia respectivă este uneori inclusă în text.

NIE cu privire la anumite subiecte de importanţă deosebită sunt elaborate anual (sau la alte intervale regulate de timp); alte subiecte sunt analizate în urma unor solicitări precise, venite fie din interiorul comunităţii de informaţii, fie de la alte organisme guvernamentale, cel mai frecvent de la Consiliul Naţional de Securitate (NSC). În urma unor solicitări urgente, pot fi elaborate estimări mai concise, referitoare la subiecte de interes imediat, cunoscute sub denumirea de NIE speciale (sau SNIE).

Spre deosebire de practica americană, în Israel, anterior războiului de Yom Kippur din 1973, estimările erau realizate exclusiv de direcţia de informaţii militare, un departament din cadrul forţelor armate. Deşi existau şi alte servicii de informaţii – Institutul central pentru Informaţii şi Securitate (Ha-Mossad), care desfăşura operaţiuni secrete în alte ţări, Shin Beth, care răspundea de contrainformaţii şi antiterorism, şi departamentul de cercetări al Ministerului de Externe – doar direcţia de informaţii militare avea acces la toate informaţiile şi răspundea de analizarea şi transmiterea acestora. Mai mult, membrii cabinetului nu aveau experienţă în activitatea de informaţii şi nu exista nici un mecanism prin care conducerea politică să dispună direcţiei de informaţii militare să furnizeze evaluări pe anumite teme. Această concentrare a puterii a fost criticată ulterior, considerându-se că a contribuit la eşecul serviciilor israeliene de informaţii, care nu au anticipat atacul egipteano-sirian din 6 octombrie 1973 (subiect analizat în secţiunea "eşecurile serviciilor de informaţii" din acest capitol).[49]

Diferenţieri între serviciile de informaţii

Dacă funcţiile legate de informarea curentă şi de bază par a fi esenţiale pentru activitatea serviciilor de informaţii din orice ţară, în ce măsură se regăseşte însă funcţia estimativă în activitatea de informaţii? Importanţa acesteia diferă de la o ţară la alta şi de la o perioadă la alta. De exemplu, în Statele unite, elaborarea estimărilor este considerată forma supremă a activităţii de informaţii. În schimb, în Uniunea Sovietică, în anii '30, Stalin dorea să deţină controlul asupra funcţiei estimative; el a dispus NKVD (precursor al KGB) să nu îi trimită estimări sau evaluări ale situaţiei externe, ci să se limiteze la raportarea informaţiilor secrete (rapoarte de la informatori de rang înalt) pe care le obţinea.[50] Acest subiect vizează relaţia dintre funcţia de informaţii şi funcţia decizională din cadrul unui guvern, aspect analizat în capitolul 6.

EŞECURILE SERVICIILOR DE INFORMAŢII ŞI EVENIMENTELE NEPREVĂZUTE

Tipuri de eşecuri

Atacul prin surprindere – Riscul ca serviciile de informaţii să nu evalueze corect o situaţie a existat din totdeauna în activitatea de informaţii. În secţiunea de faţă sunt analizate acele cauze ale eşecurilor care ţin de propriul aparat de informaţii; în capitolul 5 va fi analizat modul în care eşecul poate fi determinat de strategiile de inducere în eroare aplicate de un adversar.

Eşecul cel mai grav şi care se poate solda cu cele mai mari prejudicii se înregistrează atunci când are loc un atac neanticipat şi forţele militare ale ţării sunt luate prin surprindere. Într-adevăr, aşa cum s-a arătat deja, configuraţia actuală a comunităţii americane de informaţii se datorează în mare măsură eforturilor de remediere a deficienţelor pe linie de informaţii ce au condus la situaţia în care ţara a fost luată prin surprindere de atacul japonez de la Pearl Harbor, din 7 decembrie 1941.

Există numeroase lucrări care au ca subiect atacurile prin surprindere reuşite. Atacarea Uniunii Sovietice de către Germania la data de 22 iunie 1941 şi atacul egipteano-sirian asupra Israelului din 1973 (care a declanşat războiul de Yom Kippur) se numără, alături de atacul de la Pearl Harbor, printre cazurile analizate cele mai frecvent.[51] Chiar şi în timpul unui război, când este de presupus că forţele militare sunt într-o stare de mai mare alertă decât în timp de pace, se pot produce surprize de proporţii. Exemple în acest sens sunt atacul german din Ardeni, din decembrie 1944 (bătălia de la Bulge), intrarea Chinei în războiul coreean din noiembrie – decembrie 1950 şi ofensiva nord-vietnameză şi a Vietcong-ului (ofensiva Tet) asupra Vietnamului de Sud la sfârşitul lunii ianuarie 1968.[52]

Foarte asemănătoare cu neanticiparea unui atac este situaţia în care o ţară se aşteaptă la un atac, dar, din cauza unor estimări eronate cu privire la locul şi modul în care va avea loc acesta, reacţionează inadecvat. Un exemplu concludent în acest sens este reacţia Germaniei la debarcarea Aliaţilor în Normandia, la data de 6 iunie 1944 (ziua Z). Germanii se aşteptau, în mod cert, la un atac, dar erau atât de siguri că acesta va viza regiunea Pas de Calais, încât au considerat că Normandia este o diversiune şi au ratat o bună ocazie de a contraataca în forţă atunci când capetele de pod erau cel mai vulnerabile.[53]

Alte evenimente neprevăzute – Deşi un atac neanticipat poate fi evenimentul neprevăzut care afectează cel mai mult o naţiune, el nu este singurul de acest gen. De exemplu, un eveniment politic neaşteptat (cum ar fi o schimbare a alianţelor sau o lovitură de stat prin care este înlăturat un conducător cu care existau relaţii de bună colaborare) poate constitui o lovitură serioasă la adresa intereselor de politică externă ale unei ţări. Modul

în care americanii au subestimat, în 1978, problemele politice cu care se confrunta şahul Iranului şi amploarea opoziţiei faţă de regimul acestuia reprezintă unul dintre cele mai cunoscute exemple ale eşecurilor de acest gen înregistrate în activitatea de informaţii.[54]

În mod asemănător, absenţa avertizărilor cu privire la o schimbare economică majoră şi rapidă, aşa cum s-a întâmplat atunci când agenţiile de informaţii ale SUA nu au anticipat "şocul petrolului" din 1973 – o creştere rapidă a preţului petrolului pe plan mondial – poate fi catalogată, de asemenea, drept un eşec al activităţii de informaţii, în funcţie de ceea ce se consideră că intră în sfera de responsabilitate a agenţiilor de informaţii. Aşa cum s-a arătat, rolul activităţii de informaţii în privinţa problematicii economice este mai imprecis şi mai complicat decât în cazul chestiunilor politice sau militare. În orice caz, criza petrolului din 1973 este un exemplu care demonstrează complexitatea acestui tip de probleme, deoarece cauzele fundamentale erau de natură economică (preţul scăzut al petrolului de până atunci a încurajat consumul şi a descurajat activităţile de explorare şi dezvoltare), în timp ce cauza imediată era una politică (sprijinul acordat de ţările arabe furnizoare de petrol Egiptului şi Siriei în războiul de Yom Kippur din octombrie 1973).[55]

Dacă dezastrele care pot rezulta în urma confruntării cu atacuri prin surprindere pe câmpul de bătălie sunt evidente, prejudiciile provocate de neanticiparea unor evenimente politice sau economice sunt mai greu de evaluat. În mare măsură, acestea depind de măsura în care guvernul ar fi fost pregătit să ia măsuri, dacă ar fi fost avertizat şi de existenţa unor strategii care ar fi putut să evite producerea evenimentului sau să diminueze impactul negativ al acestuia.

De exemplu, nu este clar ce acţiuni ar fi întreprins guvernul SUA dacă ar fi fost avertizat în legătură cu şocul petrolului din 1973. În mod similar, evaluarea corectă a problemelor politice ale şahului ar fi fost cu totul altceva decât stabilirea măsurilor care s-ar fi putut lua în privinţa acestora; succesul primului demers nu ar fi garantat, obligatoriu, şi succesul celui de-al doilea.

Alte tipuri de eşecuri – Cele mai multe dintre eşecurile înregistrate în activitatea de informaţii presupun, mai devreme sau mai târziu, un eveniment surprinzător, dat fiind că o viziune eronată asupra lumii înconjurătoare va conduce la un moment dat, într-un fel sau altul, la apariţia unei situaţii nefavorabile neprevăzute. (Există însă şi cazuri în care, în urma unei activităţi de informaţii deficitare, o armată sau o ţară, care nu este conştientă de vulnerabilitatea unui adversar, nu a profitat de o situaţie favorabilă.[56] În situaţii de acest gen este vorba de un eşec, dar nu de o "surpriză") În orice caz, noţiunea de "surpriză" nu este probabil cea mai utilă pentru înţelegerea prejudiciilor pe care le pot provoca eşecurile serviciilor de informaţii.

Un eşec în activitatea de informaţii constă, în esenţă, în înţelegerea incorectă a unei situaţii, fapt ce determină un guvern (sau forţele sale

militare) să întreprindă acțiuni inadecvate sau contraproductive din perspectiva propriilor sale interese. Faptul că este luat prin surprindere de ceea ce se întâmplă este mai puțin important decât acela că acționează sau continuă să acționeze într-o manieră greşită. Astfel, eşecul activității germane de informații în ceea ce priveşte debarcările din Normandia din ziua Z nu a fost reprezentat atât de faptul că armata germană a fost luată prin surprindere, cât de acela că a evaluat greşit debarcările din Normandia, considerându-le diversiuni menite să distragă atenția de la invazia "reală", care ar fi vizat regiunea Pas de Calais.[57] În mod similar, principala cauză a înfrângerii forțelor ONU în Coreea de către chinezi, în decembrie 1950, a fost reprezentată mai degrabă de o înțelegere fundamental greşită a doctrinei şi tacticilor Chinei decât de o "surpriză".[58]

În plus, evenimente surprinzătoare care implică neanticiparea acțiunilor unei forțe ostile sau a şanselor de reuşită sunt consemnate, în special, în cazul țărilor aflate în defensivă, din punct de vedere strategic sau tactic. Dar şi o națiune aflată în ofensivă poate avea de suferit din cauza estimării eronate a efectivelor adversarului sau a altui factor relevant. De exemplu, atacul Aliaților asupra podului de la Arnhem, Olanda – "podul prea îndepărtat" – din septembrie 1944 a eşuat, în principal, din cauza faptului că, în condițiile unei prea mari încrederi în forțele proprii şi analizei superficiale a informațiilor disponibile, responsabilii cu activitatea de informații nu şi-au dat seama că în imediată apropiere se aflau două divizii germane de blindate.[59]

În cele din urmă, eşecurile analizate anterior implică o interpretare greşită care iese la iveală rapid după ce una dintre părți trece la acțiune. Alte eşecuri presupun estimarea incorectă a unui proces sau situații de durată, caz în care, dat fiind că nu se întâmplă nimic care să demonstreze starea reală de lucruri, este posibil ca eroarea să persiste un timp mai îndelungat. De exemplu, comunitatea americană de informații a făcut atât supraestimări, cât şi subestimări ale arsenalului strategic al fostei Uniuni Sovietice, acestea punându-şi ani de zile amprenta asupra viziunilor strategice ale SUA. Cele mai cunoscute dintre aceste erori sunt poate supraestimările de proporții referitoare la armamentul strategic al sovieticilor, care au indus americanilor senzația unei rămâneri în urmă în ceea ce priveşte numărul bombardierelor, la jumătatea anilor '50, şi în ceea ce priveşte numărul de rachete, începând cu sfârşitul anilor '50 şi până în 1961.[60] Dar cel puțin la fel de importantă a fost şi tendința, manifestată de la jumătatea anilor '60 şi până la începutul anilor '70, de a subestima ritmul în care Uniunea Sovietică îşi consolida forțele strategice.[61]

Cauzele eşecurilor

Cu excepția cazurilor în care nu pot fi obținute nici un fel de informații relevante, eşecurile din activitatea de informații sunt legate de o dereglare a procesului analitic, care determină ignorarea sau interpretarea greşită a datelor. Prin urmare, ele sunt similare erorilor specifice oricărui

demers intelectual – de exemplu, o greşeală făcută de un istoric în interpretarea unui text foarte vechi, care conduce la descrierea incorectă a unui aspect al antichităţii sau o greşeală a unui meteorolog în ceea ce priveşte evaluarea importanţei unui sistem de presiune scăzută, care conduce la o prognoză incorectă cu privire la starea vremii din ziua următoare.

În plus, anumite particularităţi ale procesului de analiză a informaţiilor pot determina şi alte eventuale erori. Deşi analiza informaţiilor este o activitate intelectuală, ea se desfăşoară, spre deosebire de activitatea unui om de ştiinţă, într-un cadru instituţional şi în conformitate cu anumite proceduri standardizate, astfel încât rezultatul final este mai degrabă produsul unui sistem decât al unei persoane. Ca atare, analiza informaţiilor este expusă anumitor probleme instituţionale specifice. În această secţiune sunt abordate unele dintre cauzele eşecurilor înregistrate în activitatea de informaţii, fiind analizate mai întâi cele de ordin instituţional, iar apoi cele care ţin mai mult de componenta intelectuală a activităţii de informaţii.

Subordonarea activităţii de informaţii factorului politic - Cauza cea mai discutată a erorilor sau subiectivismului din analiza informaţiilor este probabil legată de posibilitatea ca evaluările informative să fie făcute astfel încât conducă la rezultatele dorite de superiori şi nu la cele indicate de datele existente. Aceasta este însă o cauză din afara procesului de analiză propriu-zis (presupunând că analistul îşi dă seama că aprecierile formulate vin în contradicţie cu concluziile sale reale). În consecinţă, este vorba de o problemă ce ţine de managementul activităţii de informaţii – maniera în care se raportează serviciile de informaţiile la factorii de decizie pe care îi deservesc; acest subiect este abordat în capitolul 6, unde este analizată relaţia dintre activitatea de informaţii şi politică.

Indisponibilitatea informaţiilor la locul şi în momentul în care sunt necesare - Date fiind dimensiunile mari ale organizaţiilor implicate în culegerea şi analizarea informaţiilor, o posibilă sursă a problemelor o constituie faptul că informaţiile din sistem nu sunt disponibile celor care au nevoie de ele la un moment dat. Această indisponibilitate are diferite cauze: de exemplu, normele de securitate care limitează circulaţia informaţiilor secrete, luptele pentru putere dintre instituţii, în cadrul cărora controlul asupra informaţiilor se transformă într-o armă, sau simplul fapt că biroul care deţine datele nu este la curent cu necesităţile informaţionale ale altui birou.[62]

În mod similar, pot apărea probleme dacă nici un birou central nu are atât responsabilitatea realizării de analize într-un anumit domeniu, cât şi acces la toate informaţiile relevante. În cazul în care diferitele segmente ale unei probleme intră în atribuţiile unor birouri diferite, este posibil ca o informaţie esenţială să fie ignorată dacă semnificaţia ei nu poate fi înţeleasă decât în contextul tuturor datelor disponibile.

Eşecul înregistrat de activitatea de informaţii în legătură cu atacul de la Pearl Harbor se explică prin lipsa de comunicare dintre diferitele unităţi

operaţionale şi de informaţii implicate. Cu toate acestea, deşi au existat poate unele probleme de comunicare între conducerea forţelor armate şi cea a forţelor maritime din Hawai, nu este clar dacă au existat dificultăţi similare între cele două servicii şi la Washington. O problemă mai importantă a fost reprezentată de lipsa unui birou analitic centralizat, care să dispună de resursele necesare şi să răspundă de analizarea tuturor informaţiilor relevante. În schimb, se pare că informaţiile erau prelucrate "din zbor" de câteva persoane care lucrau direct pentru anumiţi factori de decizie de nivel înalt – fapt ce era o consecinţă a dimensiunii reduse a instituţiilor militare ale SUA de la vremea respectivă.

Ideile convenţionale **-** Succesul oricărui demers intelectual (de exemplu, descoperirile ştiinţifice, dar şi analiza informaţiilor) poate fi compromis de existenţa unor idei convenţionale – opinii despre un anumit subiect care sunt considerate, în general, adevărate, fără a fi însă suficient analizate. Deşi este clar că ele sunt, pe de o parte, necesare (nu se poate dedica zilnic atâta timp sau efort pentru reanalizarea şi regândirea tuturor punctelor de vedere), există riscul ca, bazându-ne pe ideile preexistente, să interpretăm eronat sau să trecem cu vederea anumite date din care reiese că lucrurile stau, de fapt, altfel.

De exemplu, în vara anului 1990, opinia vehiculată în rândul analiştilor de informaţii şi al diplomaţilor americani era că Irakul nu va invada Kuweitul. Chiar dacă fotografiile realizate din satelit indicau, la sfârşitul lunii iulie, o concentrare de proporţii a diviziilor de elită ale armatei irakiene la graniţa kuweitiană, opinia generală era că aceasta reprezenta o încercare a lui Saddam Hussein de a-i intimida pe liderii kuweitieni, în contextul disputelor privind producţia şi preţul petrolului şi rambursarea datoriilor Irakului către Kuweit. Această apreciere pornea de la premisa că, în urma războiului abia încheiat cu Iranul (1980 – 1988), Irakul era prea slăbit pentru a întreprinde o operaţiune militară amplă şi că invadarea unui stat arab de către un altul era, în orice caz, o situaţie nemaiîntâlnită. Dar, la data de 2 august, Irakul a invadat şi învins Kuweitul.[63]

Un alt exemplu al modului în care concepţiile convenţionale pot conduce la evaluarea incorectă a unui adversar este reprezentant de opinia pe care o aveau britanicii în anii '30 cu privire la reînarmarea Germaniei, care urma să fie, apreciau ei, limitată ca amploare. Potrivit lui Wesley K.Wark,

> în general, [britanicii] se aşteptau ca reînarmarea forţelor germane să depăşească limitele prevăzute în tratatul de la Versailles, dar numai până la un nivel care să răspundă cerinţelor de securitate naţională. Prin urmare, se considera că încălcarea prevederilor de la Versailles nu indica vreo intenţie agresivă… Pe lângă ipoteza generală că obiectivele Germaniei în materie de reînarmare erau limitate şi aveau un scop defensiv, se considera că ritmul reînarmării urma să respecte principiile de eficienţă. În opinia britanicilor,

> aceasta însemna că reînarmarea Germaniei va avea loc într-un ritm moderat, în vederea asigurării unor standarde înalte de profesionalism şi a celei mai bune utilizări a sistemelor de armament. Această viziune tradiţională asupra reînarmării, care demonstra o înţelegere limitată a dinamicii naziste, a fost poate cea mai însemnată dintr-o succesiune de subestimări ale capacităţii militare a Germaniei.[64]

Impactul nefavorabil al ideilor convenţionale asupra raţionamentului individual poate fi amplificat de mediul instituţional în care îşi realizează analiza un serviciu de informaţii. Dacă raţionamentul unei persoane poate fi influenţat de existenţa unor date deosebit de clare, care contrazic modelul preexistent, sau chiar de o intuiţie de moment, care indică necesitatea unei alte interpretări a datelor, este puţin probabil ca mai multe persoane să fie influenţate simultan în acelaşi fel. Astfel, cei care contestă concepţia convenţională vor întâmpina probabil rezistenţă din partea unui număr mult mai mare de persoane, care o acceptă în continuare.

Dacă o persoană face economie de timp şi efort prin faptul că nu îşi reanalizează în mod constant toate opiniile, se poate spune că şi o organizaţie procedează în aceeaşi manieră. Având în vedere dimensiunile şi complexitatea organizaţiilor implicate şi necesitatea obţinerii acordului, cel puţin tacit, al unui număr mare de persoane asupra concluziilor la care s-a ajuns, reevaluarea datelor în vederea revizuirii tuturor ipotezelor de bază este un proces foarte dificil şi de durată.

Astfel, dacă un analist trebuie să elaboreze un raport, el va studia mai întâi ceea ce s-a scris în anul anterior şi va face apoi o simplă actualizare. În felul acesta nu numai că se scutesc o serie de eforturi suplimentare, ci se asigură şi un anumit grad de siguranţă. Întrucât raportul precedent a fost aprobat, în condiţiile în care analistul se limitează la efectuarea modificărilor ce decurg din datele noi, raţionamentul de bază nu mai trebuie repetat şi se reduce la minimum posibilitatea apariţiei unei contradicţii.

Evident, aceasta creează premisele unor erori în cazul situaţiilor care presupun schimbări graduale. Întrucât informaţiile sunt aproape întotdeauna disparate şi incomplete, este posibil ca acumularea unor informaţii noi să nu determine o revizuire a analizei fundamentale. Acest lucru se poate întâmpla chiar şi atunci când majoritatea datelor sugerează că ar fi mai logică utilizarea unui alt cadru. Există astfel riscul ca o viziune învechită asupra unei situaţii să supravieţuiască mult mai mult decât ar trebui.[65]

Proiectarea unei imagini simetrice – Cele două aspecte analizate anterior sunt valabile în primul rând în ceea ce priveşte analiza informaţiilor într-un cadru instituţional. O altă cauză a erorilor survenite în procesul de analizare a informaţiilor este reprezentată însă de aplicarea unui raţionament greşit, lucru care se întâmplă într-o mare diversitate de situaţii, nefiind legat de cadrul instituţional în care se desfăşoară analiza. Acest fenomen poate fi

denumit "proiectare a unei imagini simetrice", ceea ce presupune că situațiile nefamiliare sunt interpretate pe baza celor familiare.[66] În activitatea de informații, aceasta înseamnă că acțiunile unui alt stat sunt evaluate sau anticipate prin analogie cu acțiunile pe care consideră analistul că le-ar lua el (sau țara sa) dacă s-ar afla într-o situație similară.

De exemplu, faptul că serviciile israeliene de informații nu au anticipat atacul egipteano-sirian care a declanşat războiul de Yom Kippur din octombrie 1973 pare să se fi datorat, în parte, acestui fenomen; serviciile israeliene de informații nu şi-au imaginat că arabii vor declanşa un război pe care, după toate probabilitățile, l-ar fi pierdut.[67] De exemplu, cu mai puțin de două luni înainte de izbucnirea războiului, Moshe Dayan a spus Colegiului de Stat Major al forțelor israeliene de apărare că "raportul de forțe ne este atât de favorabil, încât anulează considerentele arabilor pentru o reluare imediată a ostilităților."[68]

Privind însă retrospectiv, se pare că preşedintele Egiptului, Anwar Sadat, a dorit ca războiul să pună capăt impasului în care se găseau relațiile dintre israelieni şi arabi şi nu a mizat, de fapt, pe câştigarea lui. Deşi ulterior a avut loc o răsturnare de situație pe câmpul de luptă, victoriile inițiale ale arabilor (în special, traversarea de către egipteni a Canalului Suez şi ruperea aliniamentului de apărare al israelienilor) au asigurat contextul psihologic pentru recâştigarea, în cele din urmă, a Peninsulei Sinai. Ignorarea posibilității de asumare a unor astfel de riscuri, străină experienței militare israeliene şi americane, poate reprezenta un exemplu de proiectare a unei imagini simetrice.

Un alt exemplu concludent poate fi găsit în raportul Comisiei Church, o comisie specială a Senatului SUA, înființată în 1975 pentru investigarea comunității de informații. În raportul respectiv este citat următorul paragraf dintr-un proiect al estimării naționale de securitate din 1969, referitor la forțele nucleare ofensive ale Uniunii Sovietice:

> Credem că sovieticii îşi dau seama de dificultățile enorme pe care le-ar presupune orice încercare de obținere a unei superiorități strategice în măsură să modifice semnificativ echilibrul strategic. În consecință, considerăm că este foarte puțin probabil să încerce, în perioada vizată de această estimare, să ajungă la capacitatea necesară pentru a da "prima lovitură", adică pentru a lansa un atac prin surprindere împotriva Statelor Unite, fără ca URSS să înregistreze prejudicii inacceptabile. În mod aproape sigur, în opinia sovieticilor, costurile unei astfel de operațiuni, adăugându-se la costurile aferente tuturor celorlalte angajamente militare, ar fi mult prea mari. Mai important este însă faptul că, în mod aproape cert, ar considera că este imposibil să pună la punct şi să desfăşoare forțele ofensive şi defensive necesare pentru a contracara cu succes diferitele componente ale forțelor strategice de atac ale SUA. În cele

> din urmă, chiar dacă un astfel de proiect ar fi fezabil din punct de vedere economic şi tehnic, sovieticii ar ajunge aproape cu certitudine la concluzia că Statele Unite îşi vor da seama de aceste eforturi şi vor întreprinde demersuri similare sau chiar mai ample.[69]

Lăsând la o parte contextul în care Comisia Church citează acest pasaj (administraţia Nixon şi, în special, secretarul Apărării, Melvin Laird, sunt criticaţi pentru faptul că au făcut presiuni asupra directorului CIA, Richard Helms, în vederea eliminării acestui pasaj din versiunea finală a NIE, lucru care s-a şi întâmplat), raportul său nu arată dacă evaluările din pasajul respectiv se bazau pe informaţii din interior despre viziunea strategică a Kremlinului. Într-adevăr, din modul de exprimare (de exemplu, "în mod aproape sigur") reiese că este vorba de opiniile analiştilor în legătură cu viziunea sovieticilor şi nu de date obţinute direct din documente sau de la informatori de nivel înalt.

Ca atare, este un exemplu de proiectare a unei imagini simetrice, nu numai prin prisma celor trei afirmaţii (ultimele trei fraze) pe care le prezintă în susţinerea ideii sale principale, ci şi prin întreaga manieră de tratare a problemei. Prima afirmaţie conduce la ideea că serviciile americane de informaţii ar fi ştiut ce nivel de cost ar fi fost considerat prohibitiv de către sovietici, apreciere care se baza, în principal, pe proiectarea unei imagini simetrice – Statele Unite erau cele care au ajuns la concluzia că acest obiectiv nu era fezabil din punct de vedere economic. A doua afirmaţie reflectă o idee larg răspândită în rândul strategilor americani, dar care nu era neapărat împărtăşită la momentul respectiv de teoreticienii sovietici din domeniul militar. În cele din urmă, cea de-a treia afirmaţie atribuie sovieticilor o viziune mecanicistă, apolitică asupra cursei înarmărilor (de tipul acţiune – reacţiune), care predomina în Statele Unite, dar nu neapărat şi în Uniunea Sovietică.

Şi mai important este poate faptul că modul în care este pusă problema în primele două fraze – echivalându-se "superioritatea strategică în măsură să modifice semnificativ echilibrul strategic" cu "capacitatea necesară pentru a da prima lovitură" – reflectă doctrina SUA privind distrugerea reciprocă (MAD), fără a se face vreo încercare de a înţelege ce anume considerau sovieticii la vremea respectivă a fi semnificativ. Reiese astfel că sovieticii ar considera că soluţiile parţiale la problema contracarării forţelor strategice ofensive ale SUA sunt nesemnificative şi nu merită să fie puse în practică.

Dat fiind însă că această opinie este doar implicită şi nu exprimată, ea nu este analizată în baza unor date concrete. (De exemplu, o evaluare atentă a acestei opinii ar fi trebuit să aibă în vedere accentul pus de sovietici pe apărarea antiaeriană strategică, existenţa unor adăposturi subterane pentru factorii de conducere şi sistemul de apărare împotriva rachetelor balistice de la Moscova, chiar şi în absenţa unui astfel de sistem la nivel naţional). Faptul că această viziune a fost atribuită sovieticilor pare să fie un caz de proiectare

a unei imagini simetrice de către analişti, care considerau că logica ce stătea la baza viziunii americane era imbatabilă şi, ca atare, era împărtăşită şi de sovietici.

O altă formă des întâlnită de proiectare a unei imagini simetrice, care afectează capacitatea de evaluare corectă a progreselor ştiinţifice sau tehnologice realizate de un adversar în domeniul militar, este sindromul "aici nu s-a inventat". Acest sindrom se caracterizează prin faptul că nu se ia în serios posibilitatea ca un adversar să fi realizat o armă sau un dispozitiv la care propriul sistem tehnico – militar nu s-a gândit sau l-a considerat lipsit de fezabilitate ori eficienţă. Acest sindrom se face simţit mai ales atunci când este vorba de un adversar considerat inferior din punct de vedere tehnologic.

R.V.Jones analizează acest fenomen atunci când prezintă activitatea de informaţii desfăşurată de britanici pe linie tehnico-ştiinţifică în perioada celui de-al doilea război mondial. Într-o concluzie formulată pe marginea unui raport informativ privind racheta balistică V-2, pe care germanii au realizat-o spre sfârşitul războiului şi au lansat-o pentru prima dată asupra Londrei, la data de 8 septembrie 1944, Jones trece în revistă cele patru posibilităţi legate de o realizare tehnică: în acest caz, britanicii fie reuşesc, fie nu reuşesc în privinţa ei, iar germanii, la rândul lor, reuşesc sau nu. Sindromul "aici nu s-a inventat" se materializează atunci când

> specialiştii noştri fie eşuează, fie nu încearcă, [iar] germanii reuşesc. Acesta este cel mai interesant caz din activitatea de informaţii, dar este greu de depăşit prejudecata că, întrucât noi nu am realizat un lucru, acesta este imposibil sau absurd. Pe de altă parte, atunci când analizează realizarea germanilor, specialiştii noştri se transformă, de fapt, în novici şi, ca atare, pot emite ipoteze mai hazardate decât cele ale serviciilor de informaţii [adică ale analiştilor de informaţii care nu sunt specialişti în tehnologia respectivă], care au cel puţin avantajul unui contact mai apropiat cu inamicul.[70]

Soluţia oferită de Jones la această problemă este ca analistul de informaţii să trateze cu prudenţă opiniile specialiştilor din domeniul tehnic, încercând totodată să valorifice competenţa acestora:

> Serviciile de informaţii trebuie să se ţină seama întotdeauna de faptul că recomandările vin din partea unui specialist britanic, şi nu german. Dacă nu se are în vedere permanent această distincţie, se pot face erori grave. În domeniul militar, Napoleon era perfect conştient de acest risc, făcând referire la "construirea unei imagini a inamicului". Acelaşi risc există şi în domeniul tehnic.[71]

“Soluţii” la problema eşecurilor din activitatea de informaţii

Ce este eşecul? Mai frecvent decât ar fi de aşteptat, având în vedere mitul omniscienţei serviciilor de informaţii, se întâmplă ca rapoartele sau estimările informative să conţină afirmaţii eronate şi să aibă loc evenimente importante, fără ca agenţiile de informaţii să le fi anticipat. Pentru a stabili dacă situaţiile de acest gen constituie sau nu eşecuri ale activităţii de informaţii, este necesar un etalon în funcţie de care să fie evaluate performanţele pe linie de informaţii.[72] Se consideră adesea că activitatea de informaţii ar trebui evaluată în raport cu un ideal de clarviziune. Se pierde însă din vedere că activitatea de informaţii implică, în general, o confruntare reală cu un adversar uman, şi nu o luptă metaforică cu natura (aşa cum se întâmplă în cazul cercetării ştiinţifice, care încearcă să determine natura să îşi dezvăluie secretele).

De exemplu, incapacitatea victimei de a anticipa un atac prin surprindere este reversul succesului repurtat de atacator în ceea ce priveşte surprinderea adversarului. În activitatea de informaţii, una dintre părţi încearcă, de cele mai multe ori, să zădărnicească eforturile făcute de adversar pentru înţelegerea corectă a situaţiei. În acest scop, ea va face uz de o multitudine de tehnici de informaţii, inclusiv de diversiuni, după cum se poate vedea din capitolul 5, în care este abordată activitatea de contrainformaţii.

Prin urmare, progresele înregistrate în privinţa tehnicilor utilizate în activitatea de informaţii nu pot fi comparate, de exemplu, cu cele din domeniul chimiei. În urma progresului înregistrat de cercetările din domeniul chimiei şi a răspândirii noilor concluzii la care s-a ajuns, chimiştii din întreaga lume pot obţine rezultate mai bune în activitatea lor. În domeniul informaţiilor, lucrurile nu stau însă la fel; faptul că datele sau procedurile de dată recentă permit unui grup de ofiţeri de informaţii să obţină rezultate mai bune înseamnă, de regulă, că adversarii acestora nu îşi mai îndeplinesc atribuţiile la fel de bine ca până atunci şi, într-un fel, înregistrează eşecuri. Acest lucru este valabil mai ales în privinţa acţiunilor deliberate de luare prin surprindere, dar are o arie mai largă de cuprindere.[73]

Ducând lucrurile la extrem, eşecurile din activitatea de informaţii pot fi considerate similare celor din jocul de şah. Evident, pentru perfecţionarea abilităţilor de şahist, este normal să se analizeze cât mai amănunţit stilurile de joc şi mutările individuale. În felul acesta, ar trebui să se îmbunătăţească calitatea jocului individual şi, în cazul în care cunoştinţele dobândite sunt împărtăşite şi altora, aceştia vor juca la rândul lor mai bine. Per ansamblu, nu poate avea loc o creştere a numărului de jocuri de şah câştigate în raport cu numărul celor jucate. Desigur, în calitate de cetăţeni, nu ne interesează o activitate de informaţii mai performantă la modul general, ci încercăm să consolidăm capacitatea pe linie de informaţii a ţării noastre şi, în felul acesta, să o minimizăm pe cea a adversarilor.

Soluții instituționale. Printre soluțiile instituționale avute în vedere cel mai frecvent – soluții care presupun restructurarea cadrului instituțional în care se desfăşoară activitatea de informații – se numără *analiza competitivă* şi crearea unui "*avocat al diavolului"*.

"Analiza competitivă" se referă la crearea unor centre analitice distincte în cadrul guvernului, fiecare dintre ele având dreptul de a formula şi transmite propriile evaluări informative. În principiu, fiecare centru ar urma să aibă drepturi egale şi generale de acces la datele neprelucrate, indiferent de agenția de informații care le-a obținut. (În practică, dat fiind caracterul secret al anumitor tipuri de informații - de exemplu, informațiile care ar putea conduce la identificarea unei surse umane - acest lucru poate fi greu de realizat.)

De regulă, toate aceste centre sau unele dintre ele sunt părți componente ale unor departamente şi agenții guvernamentale importante sau ale unor servicii militare şi funcționează, în primul rând, pentru a răspunde nevoilor speciale de informații ale organizațiilor cărora le aparțin. De exemplu, în Statele Unite, Agenția de Informații a Apărării face parte din Departamentul Apărării şi este subordonată atât şefilor Statului Major Reunit, cât şi Secretarului Apărării; fiecare serviciu militar are propriul comandament sau serviciu de informații; Departamentul de Stat are propriul Birou de Informații şi Cercetare. Într-o anumită măsură, competiția dintre ele reflectă faptul că sunt subordonate unor departamente guvernamentale diferite, care uneori se află la rândul lor în competiție.

Există, de asemenea, şi posibilitatea înființării mai multor centre analitice ad-hoc care să investigheze aceeaşi problemă. Două exemple de acest gen, care au fost date publicității, sunt cel al Echipelor A-B din 1975-1976 şi al Comisiei Rumsfeld din 1998. În primul caz, a fost creată o echipă de experți (Echipa B) care să analizeze ultimele evoluții ale strategiei sovietice şi să confirme sau să infirme concluziile autorilor estimării naționale de securitate din anul precedent (Echipa A).[74]

În cel de-al doilea caz, o comisie condusă de Donald Rumsfeld a evaluat posibila amenințare cu rachete balistice la adresa Statelor Unite venită din partea altor țări decât Rusia şi China. Comisia a fost înființată în urma unei suspiciuni manifestate de membrii Congresului şi de alți factori de decizie, potrivit căreia o estimare națională de securitate anterioară fusese prea optimistă.[75]

Indiferent dacă este efectuată în mod sistematic sau ad hoc, avantajul unei astfel de analize competitive constă, în primul rând, în posibilitatea exprimării mai multor puncte de vedere la nivelul factorilor de decizie, fapt ce conduce la o intensificare a dezbaterilor şi permite să se stabilească dacă informațiile disponibile susțin fără echivoc una dintre opinii. Astfel, analiza competitivă poate reprezenta o soluție la problemele generate de acceptarea fără rezerve a concepțiilor convenționale. În condițiile existenței unor centre analitice concurente, creşte probabilitatea ca cel puțin unul dintre ele să manifeste scepticism în privința opiniilor generalizate cu privire la o anumită situație (deşi acest lucru nu este garantat), fiind, astfel, în măsură să

determine celelalte agenţii să îşi justifice poziţia. Analiza competitivă este o încercare de angajare - ţinând cont de cadrul limitat al reglementărilor privind securitatea informaţiilor - într-un schimb de idei specific unei societăţi democratice şi care are ca rezultat promovarea cunoaşterii în general.

Astfel, riscul ca aceste centre să adopte puncte de vedere părtinitoare, sub influenţa orientării strategice a agenţiilor coordonatoare sau a restricţiilor bugetare, este relativ redus. Potrivit acestei argumentări, iniţierea unei dezbateri intense la nivelul diferitelor centre va scoate în evidenţă netemeinicia punctelor de vedere care nu sunt susţinute de probe, creând, în acelaşi timp, premisele necesare pentru ca o serie de idei noi, neconvenţionale să fie luate în considerare.

Desigur, este posibil ca un anumit punct de vedere să fie adoptat într-o măsură relativ similară de diferitele structuri guvernamentale. Într-o astfel de situaţie, este puţin probabil ca simpla existenţă a unor centre analitice concurente să pună sub semnul întrebării concepţiile convenţionale, având în vedere că toate aceste centre ar fi dominate de acelaşi convenţionalism. Pornind de la această consideraţie, s-a propus crearea unui "avocat al diavolului" – altfel spus, a unei entităţi analitice având ca scop declarat contestarea punctelor de vedere general acceptate.

Echipa B şi Comisia Rumsfeld reprezintă, totodată, exemple de "avocaţi ai diavolului" constituiţi ad hoc pentru a analiza o anumită problemă, pornind de la premisa că o ipoteză anterioară legată de aceasta a fost eronată. Proiectul "avocatului diavolului" este o încercare de instituţionalizare a acestei practici şi, implicit, de evitare a controverselor de natură politică de tipul celor ce au planat deasupra Echipei B, despre care unii critici au afirmat că ar fi exercitat o presiune externă nejustificată (altfel spus, politică) asupra procesului de analiză a informaţiilor.[76]

Deşi ambele instrumente instituţionale prezintă avantaje, nici unul dintre ele nu poate fi privit ca o soluţie universală, sau, cel puţin, ca un pas în direcţia corectă. Într-un articol sugestiv intitulat "Why Intelligence Failures Are Inevitable", Richard K. Betts arată că nici una dintre soluţiile instituţionale sus-menţionate – şi nici o altă soluţie instituţională – nu poate preveni în totalitate eşecurile înregistrate în activitatea de informaţii.[77]

Chiar dacă analiza competitivă poate da glas unor opinii diferite faţă de concepţiile convenţionale, opinii care, în caz contrar, nu ar putea fi exprimate, acest tip de analiză oferă factorilor de decizie o gamă largă de puncte de vedere, ceea ce îi poate pune în încurcătură sau îi poate determina să ignore toate informaţiile primite şi să se bazeze pe propriile opinii. De asemenea, este posibil ca obiecţiile prezentate de un astfel de "avocat al diavolului" instituţionalizat să îşi piardă capacitatea de a-i determina pe ceilalţi să îşi reconsidere poziţia tocmai pentru că exprimarea unui punct de vedere diferit intră în "atribuţiile sale". Se poate ajunge, prin urmare, la un rezultat contrar celui urmărit, şi anume la situaţia în care anumite obiecţii justificate la concepţiile tradiţionale sunt ignorate deoarece sunt considerate o atitudine normală şi previzibilă.

Aceasta nu înseamnă, însă, că măsurile instituționale sunt lipsite de importanță sau că modificarea acestora nu poate fi benefică. Concluzia care se desprinde este că strategia optimă de organizare a serviciilor de informații nu poate fi stabilită fără a cunoaşte problemele sau deficiențele caracteristice aparatului de securitate națională al unei țări; stabilirea structurii organizatorice trebuie să țină cont de modalitățile optime de contracarare a tendințelor negative identificate. Aceeaşi soluție – de exemplu, analiza competitivă – poate fi utilă sau nocivă, în funcție de caracteristica generală a sistemului: dacă sistemul se caracterizează printr-un grad prea mare de convenționalism, analiza competitivă ar putea avea ca rezultat luarea în considerare a unor puncte de vedere noi; pe de altă parte, dacă există tendința de a permite problemelor politice interne să domine strategia de securitate națională, poate fi necesară consolidarea unei structuri de informații unitare, care să aducă în prim plan realitățile internaționale.

Soluții intelectuale. Avantajul soluțiilor instituționale este că pot fi implementate pe cale ierarhică, prin directive şi decizii manageriale; totuşi, aceste soluții nu atacă miezul problemei care conduce la eşecuri în activitatea de informații, şi anume raționamentul analistului. Îmbunătățirea raționamentelor nu este un aspect care să poată fi soluționat prin măsuri administrative directe. Într-adevăr, dacă încercăm să precizăm ce aspecte trebuie urmărite, nu putem stabili cu certitudine nici măcar ce înseamnă "îmbunătățirea raționamentului", în afara unui îndemn generic şi nu întotdeauna util de a fi "mai inteligent".

Deşi nu este posibilă stabilirea unor norme care să conducă inevitabil la o analiză corectă a informațiilor, ar putea fi util să încercăm să identificăm deficiențele sau erorile intelectuale care pot afecta procesul analitic, fie în plan general, fie într-un anumit moment şi spațiu. Astfel, putem cunoaşte aceste tendințe şi putem încerca să le corectăm.

Printre cauzele intelectuale ale eşecurilor înregistrate în activitatea de informații, am văzut că o greşeală importantă care trebuie evitată este tendința de a interpreta realitatea ca pe o reflexie a propriei imagini. Deşi toți analiştii de informații pot comite această eroare, ea reprezintă o problemă îndeosebi pentru comunitatea de informații din Statele Unite. Americanii sunt înclinați să creadă că toți oamenii au caracteristici similare, poate şi datorită experienței Statelor Unite în asimilarea şi integrarea cu succes a imigranților cu mentalități şi credințe religioase diferite. Astfel, analiştii serviciilor de informații din SUA riscă mai mult decât colegii lor din alte țări să evalueze şi să anticipeze acțiunile altora pornind de la ceea ce ar face ei în circumstanțe similare.

Prin urmare, o măsură importantă de natură să remedieze această eroare o constituie cunoaşterea aprofundată a altor societăți şi culturi. Studiul limbii şi istoriei unei țări, cunoaşterea tradițiilor religioase şi culturale ale acesteia pot contribui la creşterea semnificativă a capacității de valorificare a informațiilor. Trebuie întreprinse eforturi susținute pentru a evalua situația internațională nu numai din perspectivă proprie, ci şi din punctul de vedere al liderilor altor țări.

Capitolul 4

ÎN CULISE: OPERAȚIUNILE SECRETE

Din punctul de vedere al opiniei publice, acțiunile secrete – în special formele cele mai senzaționale ale acestora, cum ar fi răsturnarea unui guvern sau asasinarea liderului acestuia – reprezintă una din principalele forme de concretizare a activității de informații; cu toate acestea, în viziunea specialiştilor şi studenților din domeniul informațiilor, însăşi includerea acțiunilor secrete în definiția activității de informații este pusă sub semnul întrebării. Această problemă este determinată de faptul că acțiunile secrete presupun întreprinderea unor măsuri de natură să afecteze politica externă a unei țări, în timp ce activitățile de culegere şi analiză se limitează la furnizarea informațiilor care pot sta la baza politicii respective.

CE SUNT OPERAȚIUNILE SECRETE?

În accepțiunea dată de comunitatea americană de informații, *acțiunile secrete* reprezintă încercarea unui stat de a-şi îndeplini obiectivele de politică externă prin desfăşurarea unor activități secrete menite să influențeze deciziile unui alt stat sau evenimentele şi circumstanțele de ordin politic, militar ori social dintr-o altă țară. După cum sugerează termenul, caracteristica definitorie a unei acțiuni secrete o reprezintă caracterul ascuns sau secret al activităților respective. Totuşi, definirea exactă a caracterului secret poate varia în funcție de circumstanțe.

În unele cazuri, păstrarea secretului este absolut necesară, iar guvernele se străduiesc să ia toate măsurile necesare astfel încât detaliile sau chiar şi simpla existență a activităților respective să nu fie cunoscute decât de un cerc restrâns de persoane. Aceasta se întâmplă, de exemplu, în cazul în care o acțiune secretă vizează susținerea unui grup de conspiratori ce urmăresc pregătirea unei lovituri de stat în altă țară, prin introducerea ilegală de arme în țara respectivă. În alte cazuri, acțiunile în sine sunt cunoscute de opinia publică, dar guvernele implicate nu doresc să facă publică participarea lor la acestea. Un exemplu de acest gen îl reprezintă finanțarea în secret, de către guvernul unei țări, a unei publicații sau a unui post de radio care susține politica sa ori manifestă o atitudine ostilă față de politica adversarului său. În sfârşit, există şi situații în care o mare parte din informațiile cu privire la operațiuni sunt făcute publice, dar, din rațiuni diplomatice sau din alte motive, guvernele implicate evită să recunoască oficial participarea lor la evenimentele respective.

În Statele Unite, acțiunile secrete sunt definite în legislația actuală ca fiind "activitatea sau activitățile desfăşurate de guvernul Statelor Unite în

scopul influenţării situaţiei politice, economice sau militare din alte ţări, rolul jucat de [guvern] nefiind dezvăluit sau recunoscut public; astfel de activităţi nu includ… activitatea tradiţională de contrainformaţii… activităţile diplomatice… militare … [sau] din domeniul aplicării legii."[1]

Conform acestei definiţii, se face o distincţie între acţiunile secrete şi activitatea de culegere şi valorificare a informaţiilor din surse secrete, cu alte cuvinte, de ceea ce, în Statele Unite, este considerată baza activităţii de informaţii.[2] Diferenţa constă în faptul că obiectivul acţiunilor secrete nu este acela de a obţine informaţii, ci de a promova în mod nemijlocit obiectivele naţionale de politică externă. Din acest punct de vedere, se aseamănă într-o măsură mai mare cu alte instrumente de politică externă ale ţării, cum ar fi activităţile diplomatice sau operaţiunile militare, decât cu activitatea propriu-zisă de informaţii. Pe de altă parte, având în vedere că este vorba de o activitate desfăşurată în secret, care implică recurgerea la sprijinul unor aliaţi sau agenţi secreţi, se aseamănă mai mult cu activitatea de culegere de informaţii din surse umane decât cu alte strategii pe care le-ar putea pune în practică guvernul unei ţări.

Chiar dacă această definiţie este, în principiu, suficient de clară, nu este în totalitate exactă. De exemplu, deşi legea exclude în mod explicit activităţile "diplomatice", "militare", "de contrainformaţii" şi "aplicare a legii" "tradiţionale" din definiţia acţiunilor secrete, nu defineşte aceste activităţi şi nici nu stabileşte linia de demarcaţie dintre ele şi acţiunile secrete. Şi acţiunile diplomatice, de pildă, au ca scop influenţarea guvernelor şi oficialilor altor ţări şi sunt, de multe ori, întreprinse în secret; de exemplu, adesea se impune ca negocierile dintre două ţări să fie desfăşurate în secret, fără ca alte ţări sau opinia publică să aibă acces la informaţii pe această temă. Este posibil chiar ca subiectul anumitor discuţii purtate cu oficiali guvernamentali dintr-o ţară să nu fie adus la cunoştinţa altor membri ai aceluiaşi guvern.

De asemenea, "activitatea de contrainformaţii" presupune recurgerea la serviciile unor agenţi dubli, după cum vom vedea în capitolul următor. Aceşti agenţi urmăresc să obstrucţioneze eforturile adversarului de culegere de informaţii din surse umane, dar pot fi utilizaţi şi pentru a-i transmite acestuia informaţii false, menite să îl inducă în eroare şi chiar să îl determine să îşi modifice planul de acţiune. (Agentul dublu trebuie să îşi înşele adversarul în privinţa activităţilor sale, fapt ce influenţează, în mod inevitabil, activitatea de culegere de informaţii a adversarului.) Nu este clar în ce moment această activitate "tradiţională" ar trebui să fie privită nu ca o activitate de contrainformaţii, ci ca o acţiune secretă.

În plus, trebuie remarcat că termenul "acţiune secretă" pare a fi o invenţie americană, el neexistând în vocabularul altor servicii de informaţii.[3] De exemplu, cel mai apropiat echivalent sovietic al acestui termen - "măsuri active" *(aktivnye meropriiatiia)* - avea un sens mai larg decât cel al acţiunii secrete: se referea atât la "tehnicile deschise, cât şi la cele secrete, aplicate în vederea influenţării evenimentelor, strategiilor şi acţiunilor altor ţări".[4] Conform acestei definiţii, măsurile active nu intrau în totalitate în sfera

activității de informații. În schimb, includeau alte activități de politică externă desfăşurate atât de guvernul sovietic (de exemplu, activități diplomatice şi utilizarea unor mijloace de informare în masă oficiale, cum ar fi Radio Moscova), cât şi de Partidul Comunist al Uniunii Sovietice (întreprinse, de exemplu, cu sprijinul partidelor comuniste din alte țări sau al unor grupări de fațadă precum World Peace Council). Termenul punea un accent mai mare pe obiectivul urmărit – influențarea situației politice – decât pe caracterul secret sau deschis al mijloacelor utilizate.[5]

Indiferent de terminologia utilizată, este important să reținem că ceea ce Statele Unite înțeleg prin acțiune secretă reprezintă doar una din numeroasele strategii de politică externă posibile. Datorită caracteristicilor sale unice, a suscitat de-a lungul timpului dezbateri aprinse, situându-se în primplanul atenției generale; totodată, având în vedere caracterul său secret, ridică o serie de semne de întrebare în cazul unui guvern democratic. Se poate spune că alegerea termenului este, oarecum, nefericită, întrucât scoate în evidență o caracteristică a mijloacelor utilizate (caracterul secret al acestora), ignorând faptul că scopul urmărit este, sau ar trebui să fie, cel de îndeplinire a obiectivelor de politică externă. Din cauza accentului pus pe formă, în detrimentul obiectivului urmărit, dezbaterile desfăşurate în Statele Unite pe marginea acțiunilor secrete s-au concentrat, în principal, asupra legalității şi asumării răspunderii, fiind trecute sub tăcere alte aspecte fundamentale, referitoare la obiectivele şi strategia de politică externă.

În acest capitol, acțiunile secrete vor fi tratate atât ca o componentă a activității de informații, cât şi ca un instrument de politică externă; în capitolul 6, vor fi abordate aspectele specifice referitoare la desfăşurarea de acțiuni secrete de către un guvern democratic. Ținând cont de ambiguitatea definițiilor trecute şi actuale ale acțiunilor secrete, în continuarea prezentului capitol vor fi analizate activitățile cu o sferă de aplicare mai vastă decât acțiunile secrete, pentru a clarifica limitele acestora din urmă. O definiție mai satisfăcătoare a acțiunilor secrete ar trebui să se detaşeze într-o mai mare măsură de inconsecvențele legislative şi procedurale din Statele Unite; o astfel de definiție nu a fost, însă, identificată până în prezent.

TIPURI ŞI EXEMPLE DE ACȚIUNI SECRETE

În sensul său cel mai larg, acela de influențare prin mijloace secrete a evenimentelor sau circumstanțelor dintr-o altă țară, termenul "acțiune secretă" include o gamă largă de activități, de la cele prozaice, de genul acordării de asistență tehnică secretă (ca, de exemplu, cursuri de perfecționare sau furnizarea de echipamente de comunicații sau asigurarea securității) unui guvern străin prieten, până la cele mai spectaculoase, cum ar fi asasinarea unui lider sau instigarea ori sprijinirea unei lovituri de stat. Este, aşadar, dificil de redactat o listă completă cu tipurile de acțiuni secrete desfăşurate de agențiile de informații. În plus, agențiile de informații din Statele Unite nu au dezvoltat o tipologie standard a acțiunilor secrete şi nu

dispun de personal specializat care să analizeze această chestiune. În continuare vom încerca să elaborăm o astfel de clasificare.

Scopul acțiunilor secrete este de a influența acțiunile unor guverne străine sau evenimentele ori circumstanțele dintr-o altă țară. Aceste acțiuni pot viza guvernul țării respective, populația în general sau un anumit segment al acesteia. În țările democratice, efectele acțiunilor de influențare a populației sunt, de cele mai multe ori, resimțite şi de guvernul țării respective; pe de altă parte, astfel de acțiuni pot avea importante consecințe pe termen lung în țările ne-democratice sau cu sisteme totalitare.

Influențarea strategiilor, evenimentelor sau circumstanțelor din alte țări constituie însăşi esența politicii externe; acțiunile diplomatice urmăresc, în aceeaşi măsură ca acțiunile secrete, îndeplinirea acestui obiectiv. Este, de asemenea, posibilă trimiterea sau staționarea de trupe militare pe teritoriul altui stat în scopul influențării strategiei acestuia; aceasta este o măsură obişnuită pe timp de pace, dar poate fi aplicată şi în timp de război. Prin urmare, nu este surprinzător faptul că multe dintre tehnicile de acțiune secretă analizate mai jos pot fi puse în practică şi prin mijloace nesecrete. Ce este sau nu considerată acțiune secretă, din punctul de vedere al guvernului SUA, depinde adesea mai puțin de natura cazului, cât de particularitățile definițiilor legale şi administrative ale acțiunii secrete.

Sprijinul secret acordat guvernului unui stat prieten

În multe cazuri, acțiunile secrete sunt întreprinse pe baza unei alianțe tacite cu persoane sau grupări care urmăresc aceleaşi obiective. Acest lucru este mai puțin dificil de pus în practică atunci când aliatul în cauză este guvernul unui stat prieten. În acest caz, acțiunile secrete pot fi limitate ***la activități lipsite de senzațional, cum*** ar fi acordarea de asistență secretă statului aliat sub forma asigurării securității personale a liderului acestuia sau a furnizării de echipamente de comunicații securizate (criptate).

Asistența care nu implică activități pe linie de informații. Există un motiv pentru care astfel de activități sunt incluse în categoria acțiunilor secrete. Sprijinul acordat guvernului unui stat prieten îl ajută să se mențină la putere şi, prin urmare, influențează cursul evenimentelor din țara respectivă. În plus, acțiunile se desfăşoară în secret, cu alte cuvinte informațiile cu privire la sprijinul acordat nu sunt făcute publice, iar, în cazul în care se produce o scurgere de informații, guvernul nu îşi va asuma public responsabilitatea. Dar astfel de acțiuni pot fi incluse la fel de bine şi în categoria acțiunilor diplomatice secrete. De fapt, termenul "acțiune secretă" se aplică, probabil, acestui gen de activitate doar dacă a fost întreprinsă de o agenție de informații; furnizarea de asistență secretă prin intermediul personalului diplomatic sau militar nu va fi, probabil, inclusă în această categorie.

Astfel de activități sunt realizate, de obicei, la scară redusă şi sunt relativ necontroversate, motiv pentru care publicarea în presa scrisă a unor

informaţii pe această temă este puţin probabilă. Totuşi, ele pot prezenta importanţă atât din punct de vedere tehnic (prin furnizarea capacităţilor necesare guvernului statului prieten, capacităţi pe care acesta nu le-ar fi putut obţine prin forţe proprii), cât şi din punct de vedere psihologic (ca o dovadă a credibilităţii şi eficienţei sprijinului acordat guvernului respectiv). Cu toate acestea, nu întotdeauna se manifestă această lipsă a vizibilităţii şi a controverselor.

În primul rând, este posibil să apară divergenţe cu privire la statele ce trebuie considerate prietene şi eligibile pentru acordarea de asistenţă, la fel ca în cazul asistenţei nesecrete. Caracterul secret nu modifică natura acestor divergenţe, dar poate crea suspiciuni în rândul oponenţilor unui program, care pot bănui că principalul motiv pentru care programul a fost ţinut secret a fost de a evita formularea de obiecţii la adresa sa.

În al doilea rând, pot apărea discuţii cu privire la tipul de asistenţă acordată, în special dacă statul beneficiar are o reputaţie îndoielnică.[6] De exemplu, în 1974, Congresul SUA a interzis acordarea de fonduri altor state pentru instruirea forţelor de poliţie; această decizie a fost adoptată pe fondul unor controverse cu privire la încălcarea drepturilor omului de către regimurile din America Latină care beneficiaseră de astfel de fonduri.[7]

Asistenţă pe linie de informaţii. Un alt tip de asistenţă acordată guvernului unui stat prieten îl reprezintă furnizarea sau schimbul de informaţii provenite din surse secrete. Având în vedere că aceasta este o activitate de rutină, nu ar trebui să fie inclusă în categoria acţiunilor secretă. În situaţiile care presupun un schimb de informaţii de o valoare aproximativ egală, scopul furnizării de informaţii către alt stat fiind acela de a primi în schimb alte informaţii relevante, această activitate ar trebui să fie inclusă, mai curând, în categoria activităţilor de culegere de informaţii decât în cea a acţiunilor secrete.

Totuşi, în situaţiile în care furnizarea de informaţii are loc într-o singură direcţie, principala motivaţie a statului care transmite informaţiile poate fi intenţia de a ajuta celălalt stat. În acest caz, activitatea respectivă poate fi considerată sprijin secret acordat unui stat prieten, având în vedere că permite unui alt stat să îşi îndeplinească anumite obiective pe care nu le-ar fi putut atinge prin mijloace proprii, şi este desfăşurată în secret.[8]

Deşi, în general, schimbul de informaţii are loc doar între state considerate prietene (statul care furnizează informaţiile consideră că bunăstarea statului beneficiar este şi în interesul său), există numeroase exemple de situaţii în care un stat a transmis informaţii altui stat care nu este considerat prieten pentru a-l determina sau provoca să adopte o anumită decizie, care să fie în interesul ambelor părţi. Această situaţie, care presupune nu atât acordarea de asistenţă altui stat cât determinarea adoptării de către acesta a unei anumite măsuri, este prezentată mai jos ca fiind o metodă de influenţare a percepţiei unui stat cu privire la poziţia sa pe plan mondial.

Influenţarea opiniilor unui alt stat

Spre deosebire de situaţiile prezentate mai sus, în care sprijinul acordat guvernului unui alt stat porneşte de la premisa că acesta poate contribui la promovarea propriilor interese, cel mai frecvent şi mai caracteristic tip de acţiune secretă vizează influenţarea opiniilor unui alt stat, în scopul modificării strategiei, evenimentelor sau circumstanţelor din ţara respectivă în folosul propriilor interese. Acest obiectiv se realizează fie prin influenţarea acţiunilor guvernului respectiv, fie prin influenţarea opiniei publice din ţara respectivă, sau a unor grupuri şi sectoare ale acesteia, independent de acţiunile guvernului respectiv şi, adesea, împotriva intenţiilor acestuia. Scopul final îl constituie influenţarea politicii guvernului respectiv sau crearea condiţiilor necesare pentru schimbarea acestuia. În această secţiune şi în secţiunea următoare este prezentat modul în care acţiunile, evenimentele sau circumstanţele pot fi afectate prin influenţarea (1) opiniilor guvernului altui stat sau (2) opiniilor anumitor sectoare ale populaţiei din statul respectiv, cu privire la aspecte de ordin politic, militar sau economic.

Agenţii de influenţă. Metoda cea mai simplă şi mai directă de a influenţa acţiunile unui guvern străin este de a recurge la *agenţi de influenţă* – agenţi a căror principală misiune constă nu în culegerea de informaţii, ci în influenţarea directă a politicii altui stat. Având în vedere că un agent care deţine o funcţie importantă în guvernul altui stat ar putea îndeplini ambele obiective, această distincţie este mai mult de natură teoretică decât practică. În astfel de cazuri, este posibil ca utilizarea unui agent cu atribuţii pe linie de culegere de informaţii în scopul influenţării politicii guvernului ţării sale să nu fie considerată acţiune secretă. Totuşi, un serviciu de informaţii ar putea să nu se arate dispus să pună în pericol o sursă utilă de informaţii, trasându-i sarcina de a încerca să influenţeze politica guvernului său dacă, prin acţiunile sale, agentul respectiv ar putea atrage atenţia asupra sa.

Agentul de influenţă poate fi un oficial guvernamental sau un membru marcant al clasei politice din ţara ţintă (altfel spus, o persoană din interior), care are acces la alţi oficiali guvernamentali, la liderii de opinie şi la mass media. Dacă agentul de influenţă este un înalt oficial din cadrul guvernului ţintă, ar putea fi în măsură să întreprindă, pe cont propriu, acţiuni în beneficiul altui stat. Totuşi, situaţia cea mai frecventă în cazul unui guvern extins este ca agentul să îşi determine colegii să adopte anumite politici care să susţină interesele altui stat. Evident, el nu poate promova în mod făţiş politicile respective admiţând că ele sunt în beneficiul unei puteri străine, potenţial ostile, ci trebuie să încerce să influenţeze opiniile colegilor săi cu privire la situaţia politică, în aşa fel încât aceştia să considere necesară susţinerea acelor strategii care avantajează statul al cărui agent este.

De exemplu, în anii ‘30-’40, serviciile de informaţii sovietice aveau câţiva agenţi care lucrau în cadrul guvernului Statelor Unite.[9] Printre cei mai importanţi se număra Harry Dexter White, angajat al Departamentului Trezoreriei. Cu timpul, White a fost promovat în funcţia de secretar adjunct

al Trezoreriei, cea de-a doua funcție ca importanță din cadrul Departamentului. Pe lângă furnizarea de informații și secrete serviciului de informații sovietic, White acționa și ca agent de influență. Astfel, în pregătirea conferinței de la Ialta dintre Stalin, Roosevelt și Churchill din februarie 1945, White a avut inițiativa redactării unei propuneri a Departamentului Trezoreriei privind acordarea unui important împrumut pe termen de treizeci și cinci de ani, cu dobândă redusă, guvernului de la Moscova și alocarea a jumătate din suma propusă de douăzeci de miliarde de dolari, pe care Germania ar fi urmat să o plătească drept despăgubiri de război. În plus, White a făcut un apel (pe aceeași linie cu poziția Uniunii Sovietice) la distrugerea totală a capacităților industriale chimice, electrice și metalurgice ale Germaniei: "În opinia mea, cea mai bună modalitate de a consolida încrederea sau neîncrederea în relațiile dintre Statele Unite și Rusia o reprezintă poziția pe care acest guvern o va adopta în privința Germaniei". Totuși, în acest caz, eforturile întreprinse de White în interesul Uniunii Sovietice au fost parțial dejucate de opoziția manifestată de Departamentul de Stat. În cele din urmă, nu s-a acordat nici un împrumut masiv, iar Germania nu a fost dezindustrializată. Cu toate acestea, Roosevelt a aprobat, conform propunerilor înaintate de White și împotriva voinței lui Churchill, valoarea despăgubirilor de război care fusese stabilită de Rusia, precum și partea ce urma să-i revină acesteia.[10]

Un agent de influență din timpul Războiului Rece a fost norvegianul Arne Treholt, oficial în cadrul Ministerului de Externe din țara sa și, timp de peste un deceniu, agent sovietic. Profitând de funcțiile deținute în minister și la Națiunile Unite, Treholt a încercat, ori de câte ori i s-a ivit ocazia, să modereze sau să modifice politicile țării sale în beneficiul Uniunii Sovietice. De exemplu, la începutul carierei sale, Treholt a fost numit într-o funcție relativ importantă în cadrul conferințelor de drept maritim și a făcut parte din delegația norvegiană care a purtat negocieri cu Moscova pe tema limitelor teritoriale și a drepturilor de pescuit în Marea Barents. Potrivit unei relatări, "Treholt nu numai că a informat permanent KGB-ul cu privire la poziția Norvegiei în cadrul negocierilor, dar a acționat și ca agent de influență în echipa norvegiană de negociatori", contribuind la elaborarea unui tratat "care a fost aspru criticat în Norvegia pe motiv că favoriza interesele Uniunii Sovietice". În general, Treholt a făcut uz de diferitele funcții deținute în cadrul ministerului pentru a promova o serie de politici – cum ar fi cea a unei Zone Nordice Libere de Arme Nucleare – care susțineau eforturile Uniunii Sovietice vizând îndepărtarea Norvegiei de Alianța Nord-Atlantică (NATO). Treholt a jucat un rol deosebit de important în relația cu presa norvegiană, utilizându-și numeroasele contacte din mass media pentru a promova o atitudine anti-americană și anti-NATO. Când a fost arestat, în 1984, Treholt era șeful biroului de presă și comunicare din cadrul Ministerului de Externe.[11]

Un alt agent de influență din timpul Războiului Rece, recrutat din afara aparatului guvernamental, a fost Pierre-Charles Pathé, cetățean francez cu relații importante în cercurile politice, care, în 1979, a fost găsit vinovat

de spionaj în favoarea Uniunii Sovietice şi condamnat la cinci ani închisoare. Fiind un apropiat al cercurilor politice, deţinea multe informaţii despre politica desfăşurată la nivel înalt, precum şi despre viaţa personală a multor oameni politici, chiar dacă nu avea acces la informaţii secrete. Totuşi, se pare că adevărata sa infracţiune nu a fost spionajul, ci acţiunile întreprinse în calitate de agent de influenţă.

În 1976, beneficiind şi de o finanţare primită de la KGB, a lansat un newsletter politic ce purta numele *Synthèse* (Sinteza). Pe parcursul următorilor trei ani, această gazetă, care era citită de o mare parte din elita politică a Franţei (la un moment dat, 70% din membrii Camerei Deputaţilor erau abonaţi ai gazetei), a denigrat şi atacat interesele şi politica occidentală, diferenţele foarte mari dintre interesele şi politica Franţei şi a celorlalte state membre ale Alianţei Nord-Atlantice (în special, ale Germaniei Federale şi Statelor Unite) şi a susţinut poziţia URSS şi a aliaţilor săi. Pathé a fost arestat după ce a fost surprins în momentul în care primea bani de la un ofiţer KGB cu ocazia unei întâlniri clandestine ce a avut loc într-o suburbie a Parisului.[12]

Natura relaţiei dintre un serviciu de informaţii şi un agent de influenţă variază în funcţie de circumstanţe. În cazul unei persoane ca Pathé, prestigios jurnalist şi apropiat al cercurilor politice, a cărui simpatie pentru Uniunea Sovietică era anterioară oricărei relaţii clandestine cu KGB-ul (probabil că el a fost remarcat de KGB după publicarea, în 1959, a unui articol în favoarea Uniunii Sovietice), relaţia era, probabil, una flexibilă, bazată pe interese comune, nu una rigidă, bazată pe transmiterea de instrucţiuni detaliate.

Pornind de la categoriile identificate de serviciile secrete ale fostei Uniuni Sovietice, putem distinge mai multe tipuri de agenţi de influenţă, în funcţie de gradul şi tipul de control exercitat asupra acestora de serviciul de informaţii. Din prima categorie fac parte "persoanele de încredere" – cu alte cuvinte, persoanele care sunt dispuse să colaboreze cu un guvern străin pentru a promova anumite obiective pe care le împărtăşesc, dar care nu sunt receptive la primirea de instrucţiuni detaliate şi, în general, nu sunt remunerate. O altă categorie este cea a agenţilor "controlaţi", care primesc şi execută ordine precise şi care, de obicei, primesc o recompensă bănească pentru serviciile lor. La polul opus se află persoanele care sunt manipulate (de pildă, prin intermediul unor consilieri sau al unor persoane din anturajul său) să întreprindă anumite acţiuni în interesul altui stat, dar care nu sunt conştiente de manipularea la care sunt supuse.[13]

Informarea şi dezinformarea. O altă metodă de influenţare a acţiunilor unui stat constă în furnizarea anumitor informaţii (veridice sau false) menite să îl determine să întreprindă un anumit gen de acţiuni. Un exemplu de astfel de caz este cel petrecut în 1983, când Statele Unite i-au transmis Aiatolahului Komeini informaţii cu privire la "prezenţa unor agenţi şi colaboratori sovietici în Iran". Această informaţie a avut ca rezultat două sute de execuţii şi "desfiinţarea partidului comunist Tudeh", fapt ce "a dat o

lovitură majoră operațiunilor KGB şi influenței sovietice" în Iran. Statele Unite obținuseră, se pare, această informație de la un "diplomat" sovietic din Teheran, Vladimir A. Kuzichkin, care a imigrat în Marea Britanie în 1982; Kuzichkin era, de fapt, "un ofițer superior KGB…care avusese misiunea de a ține legătura cu partidul Tudeh".[14]

Deşi, în acest caz, CIA a fost, se pare, implicat, nu este obligatorie recurgerea la serviciile secrete pentru a transmite astfel de informații. În lipsa implicării serviciilor de informații, o astfel de activitate nu ar fi, probabil, considerată acțiune secretă, deşi natura ei ar rămâne, în principiu, aceeaşi. Un exemplu de astfel de activitate, care nu poate fi inclusă în categoria acțiunilor secrete, l-a reprezentat încercarea primului ministru britanic, Winston Churchill, în aprilie 1941, de a avertiza Uniunea Sovietică cu privire la iminența atacului Germaniei.

În contextul istoric respectiv, este uşor de înțeles de ce Stalin a pus sub semnul întrebării motivele lui Churchill. Stalin, care avea, probabil, o părere preconceptă cu privire la duplicitatea englezilor, a tras concluzia că era în interesul Marii Britanii ca relațiile dintre Uniunea Sovietică şi Germania să se înrăutățească. Churchill spera, probabil, că măsurile defensive luate de Uniunea Sovietică pe baza acestei informații ar putea fi interpretate drept o amenințare de Germania, care s-ar fi simțit obligată să îşi întărească dispozitivele militare la granița sovietică. În consecință, Stalin a considerat acest avertisment ca fiind o diversiune şi l-a ignorat.[15]

Dacă cele două exemple menționate mai sus presupun transmiterea de informații reale, dezinformarea poate da rezultate la fel de bune, atât timp cât informațiile transmise sunt plauzibile. De exemplu, în timpul războiului din Vietnam, Statele Unite au încercat să creeze impresia că o mişcare de gherilă anticomunistă acționa în nordul Vietnamului. Scopul acestei dezinformări era de a determina Vietnamul de Nord să pună la îndoială eficacitatea aparatului său intern de securitate. De fapt, aşa-numita SSPL (Sacred Sword of the Patriots League) era formată din țărani care fuseseră răpiți din Vietnamul de Nord, duşi într-un sat aparent "eliberat" (de fapt, aflat sub controlul Vietnamului de Sud), îndoctrinați cu principiile SSPL, instruiți şi apoi infiltrați în Vietnamul de Nord pentru a "transmite vestea" despre ligă. Timp de patru ani, în anii '60, peste o mie de persoane din Vietnamul de Nord au fost capturate şi apoi trimise înapoi având asupra lor materiale, documente şi informații cu privire la SSPL, menite să susțină stratagema.[16]

O altă tehnică de dezinformare este aşa-numita "dezinformare tacită prin documente falsificate", care presupune transmiterea pe căi neoficiale a unui document falsificat către un guvern străin, fără a face public documentul respectiv. În cel mai bun caz, guvernul țintă (guvernul a cărui influențare se urmăreşte) acceptă documentul falsificat ca fiind autentic şi nu întreprinde alte investigații. Guvernul care se presupune că ar fi emis documentul în cauză nu ştie nimic despre acesta şi, prin urmare, nu poate să nege autenticitatea documentului.

Un exemplu de acest gen, care a eşuat pentru că guvernul ţintă a făcut investigaţii, este furnizat de Ladislav Bittman, fost agent ceh de informaţii. Potrivit relatării sale, în 1977 sovieticii au redactat un memorandum contrafăcut, care ar fi fost, se pare, emis de ambasada SUA la Teheran şi au făcut în aşa fel încât să fie transmis anonim la ambasada Egiptului din Belgrad. Memorandumul, care purta menţiunea "Strict Secret", prezenta un presupus complot pus la cale de Statele Unite, Iran şi Arabia Saudită pentru a-l răsturna pe preşedintele egiptean Anwar Sadat. Acţiunea secretă a eşuat deoarece guvernul egiptean a solicitat oficial lămuriri de la Washington şi a primit un răspuns care l-a convins că memorandumul era contrafăcut.[17]

Această formă de dezinformare poate viza direct serviciul de informaţii din ţara ţintă. În acest caz, informaţia falsă nu este transmisă guvernului ţintă, ci este lăsată, cum s-ar spune, la îndemână pentru a fi descoperită de serviciile de informaţii; de exemplu, pot fi purtate convorbiri de natură să creeze o impresie greşită, de la anumite posturi telefonice despre care se ştie că sunt interceptate de serviciul de informaţii din ţara ţintă. Acest tip de campanie de dezinformare este cunoscută sub numele de "diversiune" şi este inclusă în categoria activităţilor de contrainformaţii, nu a acţiunilor secrete. Această distincţie este, însă, oarecum arbitrară, în condiţiile în care scopul şi metoda de lucru sunt, în linii mari, aceleaşi. Pe de altă parte, o astfel de operaţiune reprezintă o modalitate de obstrucţionare a activităţilor de culegere şi analiză de informaţii desfăşurate de serviciul de informaţii din ţara ţintă; ea se bazează pe o cunoaştere detaliată a surselor şi metodelor de acţiune ale serviciului de informaţii ţintă. Din acest punct de vedere, este firească includerea sa în categoria activităţilor de contrainformaţii.

Influenţarea opiniilor populaţiei dintr-un alt stat

Spre deosebire de tehnicile prezentate până acum, cele descrise în continuare vizează în principal influenţarea opiniei publice dintr-o altă ţară. Având în vedere caracterul relativ vag al acestei sarcini, rezultatele concrete obţinute în urma aplicării acestor tehnici sunt mai dificil de evaluat. Deşi multe dintre exemple pot părea nesemnificative luate separat, efectul general pe termen lung asupra opiniei publice poate fi semnificativ. Prin urmare, aceste tehnici sunt utile în cazul în care guvernul care le aplică este conştient de faptul că se angajează într-un proces de durată şi sunt mai puţin indicate în cazul unui guvern care abordează fiecare problemă sau situaţie de criză ca pe un eveniment de sine stătător.

Agenţii de influenţă. Deşi această tehnică presupune, în mod normal, utilizarea unor agenţi care să poată influenţa, într-o manieră mai mult sau mai puţin directă, opiniile şi strategiile guvernului, există şi agenţi a căror principală misiune constă în influenţarea opiniei publice dintr-o altă ţară. Potrivit unui fost ofiţer KGB, Franţa a reprezentat un teren propice pentru acest gen de activităţi: "Majoritatea celor mai bine cotaţi agenţi

francezi de la jumătatea anilor ’70 … erau jurnalişti sau aveau relaţii strânse cu presa”. Recurgând la agenţi şi colaboratori din rândul presei franceze, serviciile de informaţii sovietice au exploatat cu succes tendinţele comuniste şi gaulliste manifestate de o parte a opiniei publice din Franţa, pentru a submina relaţiile dintre Franţa şi celelalte state membre NATO şi pentru a consolida sprijinul populaţiei în favoarea intensificării relaţiilor de prietenie cu Uniunea Sovietică.[18]

Stanislav Levchenko, maior KGB care a imigrat în Statele Unite în 1979, a relatat câteva exemple de situaţii în care Uniunea Sovietică a utilizat agenţi de influenţă pentru a influenţa presa şi strategia politică din Japonia.[19] Printre acestea se numără: utilizarea unui membru marcant al Partidului Socialist Japonez pentru a împiedica un alt membru al aceluiaşi partid, pe care KGB-ul îl credea agent chinez, să obţină o funcţie de conducere; utilizarea unui corespondent al ziarului *Yomiuri* din Tokio pentru a promova publicarea unui articol având ca scop eliberarea unui agent sovietic al serviciului de informaţii militare (GRU) care fusese arestat în urma unei operaţiuni întreprinse de un agent dublu; şi utilizarea unui tânăr corespondent american al agenţiei Associated Press pentru a publica o aşa-zisă scrisoare trimisă de soţia unui pilot al forţelor aeriene sovietice care fugise din Siberia în Japonia la bordul avionului său, MiG-25, în care aceasta îl implora, se pare, să se întoarcă în Uniunea Sovietică.[20]

Propaganda anonimă. Una dintre cele mai directe metode de influenţare a opiniei publice o reprezintă diseminarea unor puncte de vedere, informaţii sau informaţii false prin intermediul mijloacelor de informare în masă – cu alte cuvinte, prin propagandă (aşa cum este denumită peiorativ). De exemplu, ţările cu o politică externă activă au, de obicei, propriile posturi de radio (cum ar fi Vocea Americii, Radio Moscova şi altele) care exprimă făţiş opiniile acestora pe marginea unor probleme internaţionale, la fel cum editorialele exprimă punctele de vedere ale redactorului sau editorului publicaţiei respective.

Totuşi, pot exista situaţii în care un guvern nu doreşte să fie asociat direct cu materialul inclus în propagandă. În astfel de cazuri, poate pune în circulaţie anumite opinii sau relatări într-o manieră care să disimuleze originea acestora. Acest lucru este posibil fie prin inserarea acestora în publicaţii pe care nu le deţine sau controlează, fie prin includerea în publicaţii considerate de opinia publică independente, dar care sunt, de fapt, controlate de guvern.[21]

Există două motive majore pentru care un guvern poate recurge la propaganda anonimă. În primul rând, este posibil ca publicul ţintă să fie mai dispus să accepte propaganda dacă originea acesteia este disimulată, iar substratul nu este evident. De exemplu, propaganda desfăşurată de Marea Britanie în Statele Unite înainte de intrarea Americii în primul şi în cel de-al doilea Război Mondial a fost adesea diseminată prin mecanisme secrete pentru a da impresia unei relatări obiective şi independente de presă. De exemplu, recurgând la emigranţi din Europa Centrală, serviciile de informaţii

britanice au reuşit să se infiltreze în mai multe operaţiuni clandestine desfăşurate de Germania în Statele Unite. Pentru a diminua tendinţele izolaţioniste şi a provoca antipatia opiniei publice americane faţă de Germania, informaţiile referitoare la aceste operaţiuni au fost transmise de britanici redactorului şef al *Providence (R.I.) Journal*. Pe baza acestor informaţii, jurnalul a publicat ulterior o serie de articole, care au fost preluate şi de alte publicaţii din Statele Unite; se pare că redactorii publicaţiilor respective au crezut că relatările erau bazate pe investigaţii prealabile întreprinse de jurnaliştii în cauză.[22]

Un al doilea motiv pentru utilizarea mecanismelor de propagandă "neagră" este că, din considerente diplomatice, un guvern poate dori să nu fie asociat cu anumite opinii pe care totuşi intenţionează să le transmită unui anumit public. De exemplu, în timpul crizei iraniene a ostaticilor din perioada 1979-1981, guvernul sovietic a adoptat o poziţie corectă din punct de vedere diplomatic, condamnând luarea de ostatici la ONU, în vreme ce postul său de radio secret, the National Voice of Iran (Vocea Naţională a Iranului) a aprobat-o pe deplin, încercând să stârnească sentimente antiamericane în Iran. [23]

În afara presei pentru propaganda "neagră", ale cărei origini trebuie să fie ascunse, se poate vorbi şi despre o propagandă "gri", ale cărei origini nu sunt recunoscute public, deşi nu sunt ascunse pe deplin sau eficient. Spre exemplu, guvernul SUA a înfiinţat Radio Europa Liberă şi Radio Libertatea în 1949, respectiv în 1951, pentru a emite în Europa de Est şi Uniunea Sovietică. Spre deosebire de Vocea Americii, aceste posturi de radio nu aveau ca scop transmiterea poziţiei oficiale a SUA, ci urmau să ofere populaţiilor vizate atât informaţii despre propriile ţări, care nu erau disponibile în presa proprie, controlată de guverne, cât şi informaţii despre Occident. Ele erau înfiinţate ca organizaţii americane private; în sprijinul acestei acoperiri, făceau chiar apeluri publice, solicitând fonduri. De fapt, aceste posturi erau conduse de către CIA. Potrivit lui Ray Cline, "CIA a organizat acest demers… considerând că posturile de radio ar fi mai eficiente dacă legătura lor cu guvernul SUA ar fi ascunsă". [24] Dar, deşi legăturile cu guvernul american nu erau recunoscute, era evident că posturile de radio făceau parte dintr-o operaţiune americană. [25]

O altă metodă de a realiza propagandă fără ca ea să fie asociată entităţii care o generează implică transmiterea de ştiri în media independentă sau scrierea şi publicarea de cărţi de către autori şi edituri care nu au legături evidente cu guvernul sau cu agenţiile sale de informaţii. De exemplu, într-o campanie bazată pe acţiuni secrete împotriva influenţelor comuniste în Europa Occidentală derulată în timpul Războiului Rece, CIA s-a folosit de o propagandă care nu putea fi atribuită unei anumite entităţi, inclusiv subvenţionând în secret publicarea de cărţi şi articole transmise prin intermediul agenţilor de influenţă ce lucrau pentru agenţiile de ştiri sau pentru ziare.

Una dintre cele mai cunoscute activități de acest gen ale CIA a fost publicarea, în diverse ziare din afara SUA, unei copii furnizate de Agenție a "discursului secret" din 1956, prin care Hruşciov condamna "cultul personalității" al lui Stalin.[26] Un alt exemplu este sprijinul acordat de CIA scrierii şi publicării lucrării *The Penkovsky Papers*, constând într-o relatare bazată pe materiale aferente cazului real al primului spion CIA în Uniunea Sovietică, de la finele anilor 1950 şi începutul deceniului 1960.[27]

O tehnică asemănătoare constă în utilizarea unei grupări paravan ca mediu de propagandă. Acest tip de grupări, deşi aparent au o răspândire largă, sunt, de fapt, sub controlul unui guvern şi se poate conta pe ele să adopte poziții corespunzătoare obiectivelor guvernului. Aşadar, ele îndeplinesc aceeaşi funcție ca propaganda care nu poate fi atribuită unei anumite entități – exprimă opinii care servesc interesele unui guvern, dar într-un format care le poate face acceptabile pentru un anumit public. Spre exemplu, înaintea celui de Al Doilea Război Mondial, britanicii au înființat mai multe grupări paravan al căror obiectiv era să combată şi să hărțuiască "America First", cea mai mare şi mai importantă organizație izolaționistă din Statele Unite.[28]

Falsurile. O altă tehnică de a pune în circulație materiale fără a-ți asuma răspunderea pentru ele este realizarea şi transmiterea de documente falsificate.[29] Ca şi în cazurile discutate anterior, această tehnică serveşte acelaşi obiectiv general: de a influența percepțiile unui public țintă, astfel încât acesta să ia măsurile dorite. Materialele utilizate în acest sens – ce pot consta în argumentele prezentate de către un agent de influență, conținutul propagandei care poate fi atribuită sau nu unei entități, ori textul falsului – trebuie să fie plauzibile pentru cei asupra cărora se încearcă influențarea. Prin urmare, în general ne aşteptăm ca în materialul fals să fie inserate elemente de adevăr, pentru ca acesta să pară mai plauzibil. Amalgamul rezultat, care are efectul de a induce în eroare publicul țintă în unele privințe semnificative, este adesea denumit "dezinformare".[30]

Desigur, este posibil ca un mesaj în totalitate adevărat (sau unul considerat adevărat de către cei care îl propagă) să aibă efectul dorit asupra publicului țintă. Cel mai eficient fragment al discursului secret al lui Hruşciov (în sensul diminuării prestigiului comunismului în Europa de Vest şi de Est) consta în dezvăluirile legate de crimele şi "cultul personalității" al lui Stalin. Publicarea acestuia a reprezentat o acțiune secretă eficientă a CIA, deşi fragmentul respectiv al textului era indiscutabil autentic. În mod similar, dezvăluirea de către britanici a telegramei originale a lui Zimmerman, despre care am discutat în capitolul anterior, a fost o lovitură de maestru a propagandei neatribuibile unei anumite entități.

Sprijin pentru forțele politice prietene

O altă modalitate de influențare a evenimentelor din alte țări este asigurarea de sprijin material forțelor politice prietene, cum ar fi partidele politice, grupurile civice, sindicatele şi presa. Deşi acest lucru se poate face şi fățiş, iar uneori chiar se face, ajutorul acordat în secret poate părea mai indicat grupărilor beneficiare, de vreme ce astfel este mai puțin probabil să apară acuzații privind ingerințe străine în afacerile interne ale țării, care să le afecteze pe plan politic.

Desigur, aşa s-a întâmplat în cazul asistenței acordate în secret de americani sindicatului polonez independent Solidaritatea, în anii 1980. Lucrând împreună cu Biserica Catolică şi cu sindicatele americane, guvernul SUA a perfectat un program care viza menținerea sindicatelor poloneze şi a mişcării democrate poloneze după ce guvernul comunist al țării declarase instaurarea stării de asediu, în decembrie 1981. Printre tipurile de asistență acordată în secret Solidarității se numărau fonduri, prese de tipar şi echipament clandestin pentru comunicații. [31]

În mod tradițional, fosta Uniune Sovietică a facilitat acest tip de activitate făcând o distincție fictivă între guvernul sovietic şi Partidul Comunist al Uniunii Sovietice. În vreme ce guvernul putea avea relații corecte din punct de vedere diplomatic cu alte state, Partidul, prin intermediul unor organizații precum Comintern, Cominform (Biroul Comunist de Informații, care din 1947 până în 1956 a transmis "linia de partid" statelor şi partidelor comuniste străine) şi Departamentul Internațional al Comitetului Central, a menținut relații cu forțele "progresiste" din întreaga lume şi le-a acordat sprijin. [32] Ca reacție la activitatea sovietică de acest gen din Europa de Vest postbelică, Statele Unite s-au implicat într-un program ce derula acțiuni secrete de susținere a grupărilor politice şi culturale democratice şi a sindicatelor. [33]

În timpul administrației lui Harry Truman (la finele anului 1947), impulsul imediat a fost teama că alegerile din Italia, programate pentru primăvara anului următor, ar putea fi câştigate de comuniști. Pentru a sprijini demersurile propagandistice fățişe ale SUA, CIA a derulat activități cum ar fi asigurarea de sprijin financiar şi de alte tipuri (de exemplu, instruire în domeniul tehnicilor de campanii electorale) partidelor politice necomuniste. De asemenea, Agenția a încercat să influențeze socialiştii să nu coopereze cu comuniştii. După cum explica Ray Cline, fost director adjunct al CIA,

> Aceste tipuri de asistență financiară şi tehnică acordate partidelor creştin-democrate sau altor partide necomuniste, cât şi eforturile de a separa socialiştii de fronturile unificate dominate de comuniști, trebuiau să se deruleze în secret. Liderii partidelor italiene nu îşi puteau permite să îi lase pe comuniști să obțină dovezi că sunt susținuți din afara țării, deoarece astfel s-ar fi redus din indignarea opiniei publice

> față de dependența financiară și politică a Partidului Comunist de Uniunea Sovietică. Prin urmare, CIA a primit însărcinarea de a transmite fondurile și asistența tehnică necesare obținerii de voturi și câștigării alegerilor. [34]

În urma reușitei electorale a partidelor necomuniste, CIA "a fost instruită să propună anumite programe de informare și alte acțiuni de natură politică pentru a neutraliza eforturile comuniștilor de a-și extinde influența politică în Europa Occidentală". [35] După cum preciza Comisia Church, programul rezultat implica "subvenții pentru organizațiile muncitorești și politice adverse", care

> aveau ca scop să servească drept alternative la grupările de inspirație sovietică sau comunistă. [Se realizau] operațiuni vaste în domeniul sindical, mediatic și electoral, la sfârșitul anilor 1940. Sprijinul pentru organizațiile "adverse", în special în activitățile vizând sindicatele, studenții sau cele culturale, urmau să capete o amploare mult mai mare în anii 1950 și 1960. [36]

După cum sublinia Ray Cline, majoritatea fondurilor ajungeau la organizații ale stângii necomuniste, care nu susțineau neapărat anumite poziții ale SUA în ce privește politica externă. El citează în particular Congresul pentru Libertate Culturală și publicații politice precum *Encounter* din Anglia și *Der Monat* din Germania de Vest. [37] Această strategie se pare că a fost dictată de opinia că principalul câmp de luptă ideologic al Europei viza forțele de stânga și că organizațiile mai conservatoare ar avea, în orice caz, mai puține probleme în a obține fonduri de pe plan intern. Totuși, ea scoate în evidență o ambiguitate tipică acțiunilor secrete: este adesea posibil să lucrezi cu oameni cu care ai divergențe de opinie majore. Problemele pe care le-ar cauza divulgarea unui astfel de aranjament devin un alt motiv pentru păstrarea secretului.

Un program SUA mai controversat de acest tip a fost realizat în Chile, după instalarea marxistului Salvador Allende în funcția de președinte, în 1970. Acest program avea ca scop să asigure partidelor politice de opoziție și presei resursele financiare necesare pentru a supraviețui în contextul haosului economic din țară și al măsurilor de reglementare ostile adoptate de către guvern. Controversa pe marginea acestui program s-a concentrat pe două aspecte (dincolo de întrebarea mai generală vizând ce poziție ar fi trebuit să adopte SUA față de regimul lui Allende).

În primul rând, programul a fost considerat inutil deoarece, conform Comisiei Church, evaluările naționale de securitate ale CIA din perioada regimului Allende indicau faptul că "în ciuda încercărilor de a hărțui și de a afecta din punct de vedere financiar presa de opoziție", aceasta (și în special *El Mercurio*, cel mai mare ziar național și cel mai important mediu care

propaga idei defavorabile lui Allende) a rămas liberă, iar "sistemul politic tradiţional din Chile a continuat să manifeste un curaj spectaculos." [38] Totuşi, comisia a observat că cei responsabili cu elaborarea acestor evaluări nu aveau cunoştinţă de programul de acţiuni secrete: "prin urmare, nu a existat o evaluare care să arate dacă aceste sectoare ar supravieţui *fără* banii proveniţi din SUA". [39]

Un alt subiect controversat a vizat scopurile pentru care Statele Unite au acordat ajutor. SUA au încercat în mod serios să nu acorde asistenţă acelor grupări care încercau în mod activ să răstoarne guvernul (cum ar fi sindicatul şoferilor de camioane, întrucât grevele prelungite şi pagubele cauzate ofereau ocazii de lovituri militare) şi să-şi limiteze ajutorul acordat la partidele de opoziţie şi la presă. Potrivit lui Gregory Treverton, un critic al acţiunilor secrete care era membru al Comisiei Church, "tiparul consfătuirilor din cadrul guvernului SUA sugerează o distincţie precisă între sprijinirea forţelor de opoziţie şi finanţarea grupărilor care încearcă să promoveze o lovitură militară. Încercarea de stabilire a acestei distincţii a fost, din câte îmi dau seama, un demers onest". [40] Cu toate acestea, după cum conchide şi Treverton, această distincţie era una eminamente artificială, care exista "numai în minţile americanilor, nu şi ale chilienilor". [41] Grupările de opoziţie îşi aleg singure strategiile pentru a-şi atinge obiectivele şi îşi selectează tacticile şi aliaţii în consecinţă; dacă diversele forţe adversare lui Allende doreau să coopereze, sprijinul SUA pentru unele dintre grupări ajungea şi la aliaţii acestora.

Influenţarea evenimentelor politice prin violenţă

În ochii opiniei publice, acţiunile secrete sunt adeseori asociate mijloacelor violente de influenţare a evenimentelor politice. După cum au demonstrat argumentele prezentate anterior, multe tehnici non-violente pot fi utilizate în secret pentru a se influenţa comportamentul politic, evenimentele şi împrejurările din alte ţări. Dar, în plus faţă de aceste activităţi care reprezintă majoritatea tipurilor de operaţiuni secrete, există şi tehnici care implică susţinerea sau utilizarea violenţei.

Sprijinul pentru loviturile de stat, "Războaiele de eliberare naţională" şi "Luptătorii pentru libertate". Sprijinul pentru grupările politice nu trebuie să fie limitat la oponenţii paşnici ai unui guvern străin, ci poate fi extins asupra grupărilor care încearcă fie să influenţeze politica guvernului respectiv prin mijloace violente, fie să îl răstoarne. Acest lucru poate implica sprijinirea unei grupări existente sau crearea unei grupări "marionetă", care să realizeze aceste activităţi. [42]

Tipul exact de sprijin acordat depinde parţial de gruparea în cauză şi de strategia adoptată de aceasta. El poate lua forma asistenţei militare acordate forţelor combatante insurgente; a sprijinului operaţional în cazul loviturilor de stat; a presiunilor politice şi economice externe, sau actelor

subversive interne îndreptate împotriva guvernelor vizate; de asemenea, se poate acorda sprijin economic sau constând în instruire pentru realizarea premiselor de pregătire a unor lupte de gherilă de lungă durată. Un exemplu în acest sens îl reprezintă cele două mari tipuri de acțiuni secrete cunoscute, în principiu, puse în practică de Statele Unite în timpul administrațiilor lui Jimmy Carter şi Ronald Reagan (sprijinul pentru luptele de gherilă împotriva regimului afgan susținut de sovietici şi sprijinul acordat contra-rezistenței în Nicaragua).

O formă deosebită a acestui tip de activități căreia i s-a acordat multă atenție o reprezintă sprijinul acordat de un stat-sponsor terorismului internațional. Sprijinul pe care îl acordă guvernele grupărilor teroriste poate diferi mult în ce priveşte amploarea şi semnificația. La limita inferioară, un stat-sponsor poate asigura facilități de instruire sau adăpost unde teroriştii să fie în siguranță şi unde să nu poată fi arestați în timp ce îşi pregătesc atacurile, sau unde să fugă ulterior. La limita superioară, acest sprijin poate include fonduri, arme, paşapoarte autentice sau false, ori utilizarea curierilor diplomatici pentru transmiterea de arme sau explozibili în țara vizată. Şi nivelul controlului exercitat de statul sponsor asupra activităților grupării teroriste poate varia; în unele cazuri, acesta poate fi destul de strict, în vreme ce, în alte cazuri, poate să nu existe, câtă vreme natura generală a activităților corespunde intereselor statului sponsor.

Forțele paramilitare. La limita dintre adevăratele acțiuni secrete şi acțiunile militare se află cazurile în care un guvern foloseşte trupe clandestine (sau voluntari) într-un conflict militar, fie de sine stătătoare, fie în alianță cu grupări similare sau cu trupe locale. Deoarece un demers la scară relativ largă de acest gen poate cu greu fi ținut secret mult timp, putem considera că acest tip de activitate ar trebui exclus din categoria acțiunilor secrete. Pe de altă parte, de vreme ce este probabil ca serviciile de informații să primească misiuni de acest gen, de obicei aceste acțiuni sunt asociate cu alte tipuri de acțiuni care presupun o mai mare confidențialitate. Totuşi, din moment ce activitatea nu va fi recunoscută public de către guvernul care o coordonează, ea rămâne o activitate secretă din acest punct de vedere, indiferent de cât de transparentă devine pretenția de neimplicare.

Acte specifice de distrugere sau violență, inclusiv asasinate. Acțiunile sub acoperire pot lua forma anumitor acte de violență, îndreptate împotriva unor persoane (cum ar fi asasinarea reprezentanților guvernelor străine, a unor figuri politice emblematice sau a teroriştilor) sau împotriva proprietății.

"Wet affairs" ("afacerile ude", eufemism pentru asasinat şi sabotaj) au fost, în diverse momente, un element obişnuit al operațiunilor serviciilor sovietice de informații. Probabil cel mai cunoscut eveniment de acest gen a fost uciderea lui Leon Troțki în Mexic, în 1940. În Statele Unite, încercările eşuate ale CIA de a-l asasina pe Fidel Castro, precum şi colaborarea acestei agenții cu forțele politice responsabile pentru asasinarea lui Patrice

Lumumba din Congo şi a lui Rafael Trujillo din Republica Dominicană au fost printre cele mai importante chestiuni care au ieşit la iveală în timpul anchetelor Agenţiei de la jumătatea deceniului 1970, ele fiind atent studiate de către Comisia Church.[43] Un rezultat al acestor dezvăluiri a fost includerea în ordinul executiv privind activitatea de informaţii al preşedintelui Gerald Ford a unei interdicţii explicite asupra "implicării sau conspirării în vederea implicării în asasinate politice".[44] Această prevedere a fost păstrată în ordinele executive privind activitatea de informaţii ale preşedinţilor Carter şi Reagan[45]. Chestiunea în cauză a fost adusă din nou în atenţia publică la finele anilor 1980, în legătură cu politica SUA în ce-l privea pe proeminentul om politic din Panama Manuel Noriega, când s-a susţinut că prevederea împiedica CIA să acorde asistenţă membrilor organizaţiei care i se opunea lui Noriega, Forţa de Apărare din Panama, pentru planificarea unei lovituri de stat (deoarece acest lucru ar fi putut implica asasinarea lui Noriega sau ar fi putut duce la acest rezultat).[46] Din acest punct de vedere, prevederea a contribuit, prin urmare, în mod indirect la invadarea de către SUA a statului Panama în decembrie 1989, ceea ce a dus la destituirea lui Noriega, dar cu un preţ mult mai mare.

Una dintre acţiunile secrete mai bine cunoscute care a implicat violenţe la adresa proprietăţilor a fost aruncarea în aer de către agenţii francezi de informaţii a vasului *Rainbow Warrior*, în 1985. Această navă, care a fost atacată în timp ce se afla în port în Noua Zeelandă, aparţinea organizaţiei de protecţie a mediului *Greenpeace*, care intenţiona să o folosească pentru a protesta împotriva testelor cu arme atomice derulate de Franţa în Pacificul de Sud şi pentru a le împiedica. Un fotograf portughez aflat la bord a fost ucis din greşeală în explozie.

Un exemplu de activitate mai distructivă de acest tip a fost campania germană secretă de sabotaj care a avut loc în Statele Unite înainte ca acestea să ia decizia de a se implica în Primul Război Mondial. Deşi poziţia lor oficială era una neutră, Statele Unite erau, totuşi, un furnizor important de muniţii şi materiale de război pentru Marea Britanie şi aliaţii acesteia în primii trei ani de conflict. Pentru a întrerupe acest flux de materiale către adversarii săi – fără a genera o reacţie a Americii îndreptată împotriva Germaniei – serviciile germane de informaţii au realizat multe operaţiuni secrete în Statele Unite. Printre acestea se numărau sabotarea vaselor care transportau provizii în Marea Britanie şi Rusia, producerea de viruşi de antrax care să fie injectaţi cailor şi catârilor trimişi în Europa şi bombardarea fabricilor de muniţie şi explozibili aflate pe Coasta de Est. Cea mai spectaculoasă acţiune a fost sabotarea căii ferate şi a terminalului maritim de la Black Tom, din New Jersey, în iulie 1916. Folosind dispozitive de incendiere şi explozibili, agenţii germani au distrus complet locul şi, împreună cu el, o cantitate impresionantă de muniţii destinate războiului din Europa. Distrugerea terminalului, poziţionat transversal faţă de Statuia Libertăţii, a zguduit Brooklyn Bridge, a spart ferestre în întregul Manhattan şi a putut fi auzită chiar şi din Philadelphia.[47]

ACȚIUNILE SECRETE ŞI PĂSTRAREA CONFIDENȚIALITĂȚII

Deşi confidenţialitatea pare a sta la baza acţiunilor secrete, importanţa şi funcţiile acesteia, după cum s-a menţionat la începutul acestui capitol, nu sunt deloc chestiuni simple; ele depind foarte mult de tipul de acţiune secretă în cauză şi de împrejurările în care este ea asumată. Gradul de secretizare necesar şi motivarea acestuia pot diferi foarte mult de la caz la caz.

În unele situaţii, păstrarea secretului poate fi absolut vitală pentru succesul operaţiunii. De exemplu, amiralul Stansfield Turner, director al Agenţiei Centrale de Informaţii în timpul preşedintelui Carter, a prezentat o operaţiune care implica trimiterea unui agent CIA la Teheran pentru a facilita eliberarea a şase americani care se refugiaseră în Ambasada Canadei, după ce se pusese sechestru asupra Ambasadei Americane, în noiembrie 1979.[48] Orice dezvăluire privind operaţiunea (chiar dacă identitatea agentului CIA şi a celor şase persoane care se ascundeau nu ar fi fost dată în vileag) ar fi pus în pericol siguranţa celor şapte oameni implicaţi, sporind atenţia iranienilor, determinându-i pe aceştia să intre în Ambasada Canadei, sau complicând procesul de scoatere a americanilor din Iran cu ajutorul unor paşapoarte false.

În mod asemănător, păstrarea secretului asupra unor detalii ale unei operaţiuni poate fi necesară pentru a împiedica apariţia de obstacole în calea acesteia, chiar dacă elementele generale ale programului sunt cunoscute. Să luăm de exemplu programul SUA de asistenţă pentru rezistenţa *mujahedinilor* împotriva Uniunii Sovietice în Afganistan, din anii 1980. Au existat mai multe ţări şi canale specifice prin intermediul cărora se transmiteau provizii rezistenţei; dacă acestea ar fi fost făcute publice la momentul respectiv, ele ar fi fost vulnerabile în faţa presiunilor diplomatice sau a sabotajului de către guvernul sovietic sau de către cel afgan.[49] Prin urmare, în ceea ce priveşte detaliile operaţiunilor secrete, este necesară păstrarea confidenţialităţii, indiferent cât de promovată este operaţiunea în întregimea sa.

Cazuri ca acestea, în care confidenţialitatea întregii operaţiuni sau a unor anumite aspecte ale acesteia este esenţială pentru ducerea ei la bun sfârşit, probabil că sunt rare. Totuşi, în multe alte cazuri confidenţialitatea este foarte importantă pentru asigurarea eficienţei operaţiunii. În această categorie considerăm că se încadrează tipurile de propagandă care nu poate fi atribuită unei entităţi sau sprijinul acordat activităţilor politice, care au fost deja discutate.

Aceste activităţi sunt îndeplinite în secret pe motiv că informaţiile transmise publicului referitoare la sursa externă a propagandei sau a fondurilor pentru activităţile de natură politică le-ar diminua efectul. De exemplu, conceptul de propagandă "neagră" constă în faptul că informaţiile care ar fi puse sub semnul întrebării sau respinse dacă s-ar şti că provin dintr-o sursă a adversarilor sau dintr-o sursă externă şi care are un motiv ascuns evident, ar fi mai uşor de acceptat dacă originea lor ar putea fi ascunsă sau atribuită altcuiva. (În multe situaţii, confidenţialitatea ar fi

necesară şi pentru că finanţarea organizaţiilor politice ar încălca legile ţării vizate).

În plus, propaganda "neagră" poate fi folosită pentru a crea disensiuni în rândul oponenţilor, prin atribuirea în mod fals a unor declaraţii sau acţiuni provocatoare. În acest caz, păstrarea confidenţialităţii adevăratei surse a propagandei este necesară pentru a i se păstra credibilitatea. Sefton Delmer, care a condus operaţiunile britanice de propagandă "neagră" în timpul celui de Al Doilea Război Mondial, susţinea că "cea mai simplă şi cea mai eficientă propagandă este să scuipi în supa cuiva şi apoi să strigi *Heil Hitler*". [50] De asemenea, multe dintre falsurile produse de fosta Uniune Sovietică erau false memorandumuri ale guvernului SUA care demonstrau o atitudine ostilă faţă de un terţ stat.

În alte situaţii, păstrarea confidenţialităţii poate fi necesară pentru a se asigura cooperarea unei terţe părţi care este dispusă să ajute numai dacă activitatea este ascunsă, pentru a evita să îşi deterioreze relaţiile externe. Din acest motiv, chiar şi în cazurile în care elementele generale ale unei activităţi secrete pot fi făcute publice fără probleme, păstrarea secretului privind aceste activităţi poate fi importantă.

O altă categorie vizează cazurile în care se evită informarea publicului nu atât pentru că aceasta i-ar pune în pericol pe cei care realizează operaţiunea sau pentru că i-ar reduce eficienţa, cât pentru că motive diplomatice fac să fie preferată nerecunoaşterea implicării guvernului. [51] De exemplu, nerecunoaşterea oficială a unei operaţiuni poate împiedica reacţia unui adversar, chiar dacă acesta deţine date de la serviciile de informaţii privind implicarea. Acest lucru este valabil în special dacă adversarul este o democraţie în care guvernul trebuie să obţină sprijinul sau înţelegerea publicului pentru orice reacţie pe care ar putea să o aibă. Adversarul poate fi împiedicat să încerce să obţină sprijinul public de teama că prezentarea dovezilor incriminatoare ar pune în pericol mijloacele cu ajutorul cărora au fost culese. Prin urmare, este firesc ca un stat care sprijină terorismul internaţional să nege că ar avea orice legătură cu un anumit eveniment de natură teroristă, chiar dacă complicitatea sa devine cunoscută.

De exemplu, capacitatea guvernului SUA de a reacţiona la atacurile teroriste cu bombă din Libia, din 9 aprilie 1986, asupra unei discoteci din Berlinul de Vest, în care un militar american şi o altă persoană au fost ucişi, depindea în mod esenţial de disponibilitatea SUA de a divulga date sensibile obţinute de la serviciile de informaţii care dovedeau implicarea Libiei. Deşi guvernul SUA a procedat astfel, a plătit un preţ mare; libienii au luat cunoştinţă de dimensiunile capacităţilor informative americane îndreptate împotriva lor şi, prin urmare, au reuşit să reducă eficienţa acestor capacităţi. [52]

În general, deşi se subînţelege că guvernele se implică în acţiuni secrete (deoarece se implică în spionaj), acţiunile secrete sunt de multe ori ilegale conform legislaţiei ţării în care au loc. De asemenea, ele pot fi şi contrare normelor de drept internaţional, la baza cărora stă principiul

neintervenției în afacerile interne ale statelor suverane, deşi acest principiu are din ce în ce mai puțină greutate în jurisprudența internațională după încheierea Războiului Rece. [53]

Din aceste motive, pentru relațiile diplomatice este preferabil să nu se recunoască o operațiune, chiar dacă țara care are de suferit de pe urma ei are cunoştință despre implicarea celeilalte. Țara vizată poate ignora acțiunile secrete, fie în interesul păstrării unor bune relații, fie pentru că nu le poate împiedica; este, însă, mult mai dificil pentru ea să procedeze astfel dacă guvernul care o conduce îşi recunoaşte public atitudinea.

Dezmințirile plauzibile

Doctrina considerată multă vreme axiomatică, potrivit căreia, chiar dacă devine cunoscută implicarea unui stat într-o acțiune secretă, şeful de stat ar trebui să poată nega că a autorizat sau chiar că a avut cunoştință despre ea, este strâns legată de cele menționate anterior. Acesta ar trebui să poată afirma, destul de plauzibil, că operațiunea a fost îndeplinită de subordonați ai săi care au acționat fără cunoştința sa ori în afara autorității sale.

În perioada postbelică, această doctrină a intrat în atenția publică atunci când, după cum s-a menționat, preşedintele Eisenhower nu a ținut seama de ea şi a recunoscut public că autorizase survolarea Uniunii Sovietice cu aeronava de recunoaştere U-2. Reacția lui Eisenhower s-a produs în mai 1960, după ce un avion U-2, anterior invulnerabil la atacuri ale forțelor de apărare aeriană datorită altitudinii mari la care zbura, a fost doborât de o rachetă sol-aer a sovieticilor în timp ce se afla într-un zbor de recunoaştere deasupra țării. (Deşi nu era vorba despre o acțiune secretă, acest incident, ce implica o aparentă încălcare a prevederilor legislației internaționale, a ridicat aceeaşi problemă a dezmințirilor plauzibile).

În biografia sa, primul secretar sovietic din perioada respectivă, Nikita Hruşciov, urma să susțină că asumarea răspunderii de către Eisenhower şi nu zborul în sine l-a determinat să grăbească întâlnirea la nivel înalt de la Paris a "Celor patru", programată să aibă loc mai târziu, în acea primăvară. [54] Totuşi, Eisenhower a considerat că nu putea să nege că ar fi avut cunoştință fără a insinua că nu controlează eficient forțele militare americane, în special dată fiind infrastructura amplă necesară susținerii zborurilor. Deşi este posibilă dezmințirea operațiunilor unui grup mic de agenți secreți, care poate fi descris ca fiind format din trădători ce acționează împotriva ordinelor sau fără ordine, tăgăduirea unei operațiuni care implica evident cooperarea multor persoane din diverse baze aviatice din toată lumea este cu totul altceva.

Un exemplu de dezmințire plauzibilă din ultimii ani este cazul agenților francezi de informații care au aruncat în aer vasul *Rainbow Warrior*. Când ofițerii francezi de informații implicați au fost arestați în Noua Zeelandă a devenit evident cui îi revine responsabilitatea pentru această situație. Guvernul francez a susținut că implicarea oficială în această situație nu a fost la nivel mai înalt decât al ministrului Apărării, Charles

Hernu, care răspundea de DGSE (*Direction Générale de la Sécurité Extérieure*, serviciul francez de informaţii externe, subordonat Ministerului Apărării). Acesta a demisionat la trei luni după atacuri. Preşedintele François Mitterrand a scăpat în principiu neatins. [55]

În Statele Unite, doctrina dezmințirii plauzibile a fost în fapt abolită de Congres în urma investigațiilor asupra chestiunilor legate de serviciile de informații de la jumătatea anilor 1970. La sfârşitul anului 1974, în urma dezvăluirilor despre un program de acțiuni secrete în Chile, Congresul a aprobat amendamentul Hughes-Ryan, care interzicea CIA acțiunile derulate în secret

> în afara situațiilor în care preşedintele constată că fiecare operațiune în parte este importantă pentru securitatea națională a Statelor Unite şi informează în timp util […] comisiile responsabile ale Congresului, inclusiv [Comisia pentru Relații Externe a Senatului şi Comisia pentru Afaceri Externe a Camerei Reprezentanților]. [56]

Atenția acordată de Congres amendamentului s-a axat pe componenta acestuia care solicita puterii executive să informeze Congresul asupra acțiunilor secrete. Totuşi, prevederea amendamentului conform căreia preşedintele trebuie să constate că acțiunile secrete propuse sunt importante pentru securitatea națională a subminat capacitatea preşedintelui de a dezminți plauzibil implicarea în orice acțiune sub acoperire care era adusă în atenția publicului. [57]

În cursul anchetei Iran-Contra, afirmațiile amiralului John Pointdexter cum că nu l-ar fi informat pe preşedintele Reagan despre transferul veniturilor obținute din vânzarea armelor iraniene către rezistența din Nicaragua au reprezentat o încercare de resuscitare a doctrinei dezmințirilor plauzibile. Mai exact, Pointdexter a depus mărturie că nu l-a informat pe preşedinte despre transferurile de fonduri, pentru a-i asigura acestuia "posibilități de a dezminți ulterior informațiile, în caz că ele ar fi făcute publice". [58]

Renunțarea la confidențialitate

Din cauza creşterii rolului de control al Congresului asupra acțiunilor secrete, Statele Unite au renunțat, în fapt, la confidențialitate în ultimii ani în cazul unor operațiuni care, în mod normal, ar fi denumite (şi încă mai sunt denumite, adesea) acțiuni secrete. De exemplu, chestiunea ajutorului acordat insurgenților din Afganistan şi Nicaragua a fost discutată deschis şi dezbătută în Congres şi în presă. Statele Unite chiar şi-au susținut, în acordul de la Geneva din 1988 privind retragerea sovieticilor din Afganistan, dreptul de a continua să acorde asistență rebelilor, câtă vreme sovieticii ajutau guvernul de la Kabul. Deşi aceste activități erau numite

acțiuni secrete, ele erau nesecrete din multe puncte de vedere. În unele cazuri, Congresul a preluat în mod deschis inițiativa de a propune acțiuni, cum ar fi asigurarea de sprijin forțelor irakiene ce se opuneau regimului lui Saddam Hussein, care în trecut ar fi fost considerate acțiuni secrete. [59]

În alte cazuri, Statele Unite au renunțat complet la confidențialitatea acțiunilor despre care s-ar fi considerat, anterior, că o impun. În 1973, de exemplu, după ce s-a confirmat public că CIA finanța Radio Europa Liberă / Radio Libertatea (RFE/RL), Congresul a înlocuit mecanismul de furnizare a fondurilor în secret cu finanțarea guvernamentală nesecretă prin intermediul unei nou-create agenții guvernamentale independente, Comitetul pentru Radiodifuziune Internațională. Deşi această schimbare nu a fost realizată voluntar, ea este posibil să nu fi avut un efect considerabil asupra credibilității RFE/RL în țările vizate. Dacă, la început, ascunderea surselor de finanțare este posibil să fi sporit eficiența RFE/RL, se pare că, în 1973, posturile de radio aveau deja o serie de realizări pe baza cărora puteau fi judecate de către public.

În mod similar, în urma discursului preşedintelui Reagan de la Londra din 8 iunie 1982, în care acesta cerea consolidarea infrastructurii democrației la nivel global, a fost înființată organizația privată cu finanțare federală *National Endowment for Democracy*, în anul 1983. Aceasta oferă sprijin nedisimulat (direct şi prin intermediul instituțiilor afiliate AFL-CIO, Camerei Americane de Comerț şi partidelor Democrat şi Republican) instituțiilor – sindicate, asociații ale oamenilor de afaceri, alte organizații civice, presă şi partide politice – care promovează democratizarea sau contribuie la o viață democratică în țările unde democrația este neconsolidată, amenințată sau inexistentă. [60]

Acest demers a fost, într-o oarecare măsură, realizat după modelul activităților internaționale ale fundațiilor politice asociate partidelor politice vest germane [61]; aceste fundații sunt finanțate de către guvernul german şi funcționează prin intermediul unor organizații politice cu viziuni similare din alte țări care au ca scop promovarea democrației. În general, se consideră că acestea au acordat sprijin, spre exemplu, partidelor necomuniste din Portugalia, în perioada turbulentă şi periculoasă ce a urmat înlăturării dictaturii lui Caetano, în 1974. Din anumite puncte de vedere, acest tip de sprijin făţiş acordat instituțiilor democratice a substituit parțial ajutorul acordat de Statele Unite în secret forțelor democratice din Europa de Vest imediat după Al Doilea Război Mondial.

ACȚIUNILE SECRETE ŞI CULEGEREA DE INFORMAȚII

După ce am trecut în revistă gama variată de activități care se încadrează în categoria acțiunilor secrete, vom analiza relația dintre acestea şi restul activităților de informații. Se ridică de la sine două întrebări. Prima: ar trebui ca acțiunile secrete să fi realizate de către agențiile care culeg

informații şi le analizează, sau ar trebui să fie integrate într-o structură birocratică separată? A doua: din perspectivă pur teoretică, acțiunile secrete ar trebui să fie considerate parte integrantă a activității de informații?

Ar trebui ca acțiunile secrete să fie independente?

Argumente împotriva existenței unei agenții independente pentru acțiuni secrete. După cum am precizat în primul capitol, atât Statele Unite, cât şi Marea Britanie au descoperit empiric faptul că existența a două organizații implicate în operațiuni clandestine – una pentru culegerea de informații (spionaj) şi una pentru acțiuni secrete – poate crea probleme importante de ordin practic. În timpului celui de Al Doilea Război Mondial, SOE (*British Special Operations Executive*), organizația abilitată de primul ministru Winston Churchill "să arunce Europa în aer", a fost separată de Serviciul Secret de Informații (SIS sau MI6) şi subordonată ministrului pentru războiul economic. Astfel au luat naştere inevitabilele rivalități interdepartamentale, deoarece ambele agenții se luptau pentru aceleaşi resurse limitate. [62]

În mod similar, în Statele Unite o componentă specială a CIA, numită Oficiul pentru Coordonarea Strategiilor (OPC), a fost înființată în 1948 pentru a realiza acțiuni secrete. Deşi din punct de vedere administrativ făcea parte din CIA, Oficiul acționa pe baza indicațiilor de strategie primite de la Departamentul de Stat şi Departamentul Apărării, iar conducătorul său era numit de secretarul de stat. [63] Acest Oficiu a fost separat de Oficiul pentru Operațiuni Speciale (OSO) al CIA, care culegea informații prin activități de spionaj. În cele din urmă, acest sistem s-a dovedit a nu fi eficient, iar cele două Oficii au fost integrate în 1952 în nou înființatul Directorat pentru Planificare. [64] Potrivit Comisiei Church, această măsură a fost determinată de (1) poziția nefirească în care se afla directorul Agenției Centrale de Informații care avea un oficiu (OPC) pentru care era responsabil din punct de vedere administrativ (şi care era finanțat prin intermediul CIA), dar care primea instrucțiuni direct de la Departamentul de Stat şi Departamentul Apărării şi (2) competiția dintre OPC şi OSO pentru serviciile aceloraşi agenți şi, dată fiind rivalitatea, dificultățile asigurării unei cooperări operative între acestea, atunci când era necesar. [65]

Deşi teoretic funcțiile lor sunt diferite, acțiunile secrete şi culegerea de informații din surse umane se bazează pe mijloace similare, în special pe cooperarea secretă dintre agenții capabili să opereze eficient în țara vizată. În multe cazuri, agenții care ar fi utili pentru realizarea uneia dintre funcții o pot îndeplini şi pe cealaltă. Se poate întâmpla foarte uşor ca două oficii separate să concureze pentru serviciile aceloraşi persoane. În plus, multe dintre funcțiile adiacente, cum ar fi asigurarea comunicațiilor între ofițeri şi agenți sau realizarea plăților clandestine, sunt asemănătoare sau identice şi necesită abilități, contacte şi resurse similare. Este necesară coordonarea strânsă pentru a se evita ca operațiunile unui oficiu dintr-o anumită țară să nu

le afecteze pe cele ale celuilalt. O astfel de coordonare poate fi greu de realizat, în special dacă ea ar impune ca interesele unui oficiu să fie subordonate intereselor celuilalt. Prin urmare, există argumente puternice în favoarea integrării acestor funcţii într-o singură organizaţie ale cărei operaţiuni în ţara sau regiunea vizată să fie controlate de un singur şef.

Argumente în favoarea existenţei unei agenţii independente pentru acţiuni secrete. Deşi din punct de vedere operativ ar fi preferabilă consolidarea acestor funcţii, s-a susţinut că natura diferită a sarcinilor implicate face neindicată această consolidare. S-a adus în special argumentul că, acordând aceleiaşi organizaţii, pe de o parte, responsabilitatea pentru implementarea politicilor (prin acţiuni secrete) cu privire la o anumită ţară şi, pe de altă parte, sarcina de culegere şi analizare a informaţiilor cu privire la acea ţară (inclusiv de evaluare a rezultatelor acţiunilor secrete), se pune în pericol obiectivitatea analizei. În principiu, acesta este acelaşi argument care a fost adus în favoarea înfiinţării unei agenţii centrale de informaţii – şi anume, să nu facă parte dintr-un minister sau departament al guvernului care trasează sau implementează strategii.

Acţiunile secrete fac parte din activitatea de informaţii?

Lăsând la o parte aspectul organizatoric, rămâne întrebarea teoretică dacă acţiunile secrete trebuie considerate a fi parte integrantă a activităţii de informaţii. Incluzând acţiunile secrete în rândul elementelor activităţii de informaţii, am subliniat că aceasta este o funcţie caracteristică a agenţiilor de informaţii; acest fapt în sine nu răspunde, însă, întrebării dacă este firesc ca, teoretic, să le considerăm parte a activităţii de informaţii. [66]

Pentru a răspunde acestei întrebări, e nevoie să înţelegem mai bine ce sunt acţiunile secrete. După cum am precizat deja, termenul în sine este luat din vocabularul specific serviciilor de informaţii din SUA şi nu are echivalente clare în uzul curent al serviciilor de informaţii din alte ţări. În plus, diversele definiţii ce i s-au dat în SUA au survenit în contextul încercărilor de reglementare a acţiunilor secrete prin lege sau prin ordin executiv; ele nu sunt neapărat utile pentru lucrarea de faţă.

Trecând în revistă tipurile de acţiuni secrete, unele (cum ar fi sprijinul acordat în secret unui regim prieten) par aproape imposibil de separat de diplomaţie, în timp ce altele (cum ar fi activitatea paramilitară) se transformă treptat în lupte de gherilă sau războaie "de intensitate redusă". Ceea ce pare a fi exclusiv acţiune secretă este calea de mijloc dintre diplomaţie şi război care implică manipularea în secret a percepţiilor celorlalţi, pentru a-i determina să ia măsuri pe care cineva le consideră în interesul său. Prin urmare, fac parte acţiunile secrete din activitatea de informaţii?

Pe de o parte, s-a susţinut că acţiunile secrete – mijloace de implementare a strategiilor – sunt foarte diferite de restul activităţii de informaţii, care se ocupă de obţinerea informaţiilor pe care trebuie să se

bazeze strategiile, fiind, prin urmare, o greşeală ca ele să fie considerate parte a activității de informații. Din acest punct de vedere, acest tip de activități sunt clasificate mai rezonabil drept unul dintre numeroasele instrumente de politică externă – cum sunt diplomația, ajutorul economic, statutul comercial de "națiunea cea mai favorizată", propaganda făţişă, programele de colaborare, programele de tipul Corpul Păcii, diplomația publică, asistența militară şi amenințarea cu utilizarea forței militare sau folosirea acesteia – pe care o națiune le foloseşte pentru a-şi promova interesele. [67]

Pe de altă parte, cele de mai sus pot fi contestate cu argumentul că definiția activității de informații drept activitate care vizează obținerea de informații este prea restrânsă: dacă obținerea de informații este atât de importantă, şi ascunderea informațiilor valoroase față de adversari trebuie să constituie o componentă importantă a activității de informații. După cum se va arăta clar în capitolul următor, o modalitate eficientă şi deosebit de profitabilă de a împiedica adversarii să afle adevărul este să îi convingi să creadă o minciună. Din această perspectivă, acțiunile secrete şi contraspionajul prezintă asemănări importante. Cel mai important, ambele pot implica influențarea comportamentului adversarului prin manipularea percepțiilor acestuia.

Întrebarea dacă acțiunile secrete fac parte din activitatea de informații este strâns legată de modalitatea de definire a activității de informații. Această chestiune va fi reluată în capitolele finale ale cărții.

Capitolul 5

SPION CONTRA SPION: ACTIVITATEA DE CONTRAINFORMAȚII

Dintre toate ramurile activității de informații, activitatea de contrainformații este, probabil, cel mai greu de definit. În linii mari, contrainformațiile se referă la informațiile culese şi analizate, precum şi la operațiunile întreprinse pentru a proteja un stat (inclusiv activitățile propriului serviciu de informații) împotriva atacurilor venite din partea serviciilor de informații adverse. Conform acestei definiții, activitatea de contrainformații are aceleaşi obiective ca şi cea de informații în sine, de vreme ce trebuie să preîntâmpine orice fel de acțiuni ale serviciilor de informații adverse.[1] Totuşi, într-un sens mai restrâns, activitatea de contrainformații se referă de cele mai multe ori strict la prevenirea culegerii de informații de către un serviciu advers, fapt ce i-ar oferi un avantaj. Vom studia mai întâi acest concept de activitate de contrainformații.

Pentru a înțelege ce implică prevenirea culegerii de informații de către un serviciu advers, trebuie să facem mai întâi de toate distincția între măsuri active şi măsuri pasive. Cele mai importante măsuri pasive, ce au ca scop împiedicarea adversarului de a culege informațiile dorite, pur şi simplu prin blocarea accesului său la acestea – construind un zid în jurul lor – poartă de obicei denumirea de "măsuri de securitate". Despre natura acestui zid – împiedicarea accesului la informații sensibile unor persoane care nu sunt de încredere, protecția documentelor şi comunicațiilor prin criptare şi depozitare în locuri sigure etc. – vom discuta mai târziu în secțiunea despre securitate. Totuşi, în primul rând, guvernul şi diversele sale departamente şi agenții trebuie să hotărască ce informațiile sunt suficient de importante pentru a fi protejate – ce informații trebuie ținute în interiorul zidului.

CLASIFICAREA INFORMAȚIILOR

Nivelurile de Clasificare

Informațiile sunt clasificate în funcție de importanța lor, adică, în funcție de pericolul pe care l-ar putea reprezenta dezvăluirea lor unei puteri adverse şi, ca urmare, importanța protecției acestora. În Statele Unite, primul sistem de protecție a documentelor privind securitatea națională a fost implementat de Departamentul de Război în 1912; Departamentul de Război şi cel Naval şi-au alcătuit propriile sisteme de clasificare în timpul celor două războaie mondiale.[3] Preşedintele Harry Truman a pus bazele primului sistem de clasificare a informațiilor la nivel guvernamental în 1951.[4]

Sistemul actual este reglementat printr-un ordin executiv promulgat de preşedintele Clinton în 1995, care stabileşte definiţii, reguli şi proceduri.[5]

Importanţa informaţiilor Sistemul de clasificare din Statele Unite încearcă să clasifice informaţiile în funcţie de gradul de atingere pe care dezvăluirea neautorizată a acestora l-ar putea aduce securităţii naţionale. Cu cât informaţia este mai importantă, cu atât mai atent trebuie protejată, iar persoanele care beneficiază de "acces" trebuie să fie cât mai puţine. În cadrul sistemului actual, nivelurile de clasificare sunt următoarele: secret, strict secret şi strict secret de importanţă deosebită, stabilite în funcţie de gradul de atingere pe care dezvăluirea neautorizată a acestora l-ar putea aduce securităţii naţionale:

- Strict secret de importanţă deosebită: "daune foarte grave"
- Strict secret: "daune grave"
- Secret: "daune".[6]

În plus, sunt folosite multe alte prevederi pentru a restricţiona accesul la informaţii. În ceea ce priveşte problemele de securitate, acestea se referă la informaţiile privind tehnicile şi resursele de culegere a informaţiilor secrete; ele sunt stabilite de directorul CIA (DCI), în conformitate cu atribuţiile sale, reglementate de Legea Naţională de Securitate din 1947, de "protejare a surselor şi metodelor secrete împotriva dezvăluirii neautorizate."[7] Totuşi, odată cu trecerea anilor, aceste clasificări (sau "compartimentări") speciale s-au înmulţit, deoarece entităţi atât din interiorul, cât şi din exteriorul comunităţii de informaţii au încercat să protejeze informaţiile considerate de o importanţă deosebită. Periodic, se încearcă sistematizarea şi controlarea acestui sistem; cel mai recent ordin executiv, de exemplu, prevede ca numărul programelor de acces special să fie menţinut la "un minim absolut", acestea fiind monitorizate de cadrele de conducere.[8] Cu toate acestea, pare o luptă fără sfârşit, iar criticile repetate privind crearea de noi clasificări confirmă motivaţia de a face acest lucru.

Nevoia de a cunoaşte După cum s-a remarcat anterior, cu cât informaţia este mai importantă (potrivit nivelului de clasificare), cu atât mai puţine persoane au acces la aceasta. În principiu, pentru a obţine acces la informaţii nu este suficient doar avizul de securitate. Persoanele care doresc să primească acces trebuie, de asemenea, să demonstreze "o nevoie de a cunoaşte" aceste informaţii în vederea exercitării atribuţiilor oficiale. Acest aspect al sistemului de control al informaţiilor este mai puţin formal decât avizele de securitate; în general, oricine gestionează informaţii clasificate este responsabil pentru confirmarea nevoii de a cunoaşte a unui solicitant înainte de a furniza informaţiile respective.[9]

Nu se ştie cu siguranţă dacă această cerinţă reprezintă o barieră eficientă împotriva transmiterii informaţiilor clasificate. În 1985, Comisia de Revizuire a Politicilor şi Practicilor de Securitate DoD, de la Departamentul

Apărării (DoD), condusă de generalul în rezervă Richard Stilwell, a constatat că "principiul potrivit căruia o persoană cu aviz de securitate beneficiază de acces doar la informațiile pe care <trebuie să le cunoască> în general nu se aplică."[10]

Ce informații ar trebui clasificate?

Cel mai simplu răspuns la această întrebare, cel puțin în ceea ce privește guvernul SUA, este oferit de definițiile informațiilor secrete, strict secrete și strict secrete de importanță deosebită de mai sus. În principiu, acestea pot părea simple, deși termenii cheie "daune", "daune grave" și "daune deosebit de grave" sunt relativ vagi, atât în sine, cât și atunci când sunt aplicați unui concept general precum securitatea națională.

De fapt, situația reală este chiar complicată. Modul în care a fost pusă problema – ce informații ar trebui protejate de accesul și dezbaterea publică – presupune o viziune fundamental liberală a guvernului și a societății, în care libera circulație a informațiilor este regula, iar împiedicarea acesteia, prin mijloace de clasificare, excepția. Probabil că această viziune constituie mai degrabă excepția, și nu regula. Până de curând, s-a aplicat doar confidențialitatea guvernamentală, eradicată doar atunci când guvernul considera că dezvăluirea anumitor informații i-ar putea aduce un beneficiu.

Gândiți-vă, de exemplu, că statele democratice publică în mod curent un volum mare de date privind bugetele pentru apărare. Deși într-o țară democratică problema clasificării bugetului total pentru apărare iese din discuție, guvernele nedemocratice obișnuiesc să facă lucrul acesta. De exemplu, guvernul sovietic considera până în 1989 că sumele alocate bugetului pentru apărare sunt secrete de stat; guvernele din China și Coreea de Nord încă mai aplică această confidențialitate.[11] Serviciile de informații din SUA alocă importante resurse pentru a stabili mărimea acestor bugete secrete pentru apărare; dacă aceste informații nu ar fi considerate importante pentru guvernul SUA, se presupune că aceste resurse ar fi alocate pentru alte operațiuni. Similar, dacă Statele Unite nu și-ar publica bugetul pentru apărare, alte servicii de informații și-ar redirecționa resursele pentru a determina mărimea acestuia, iar statele adverse ar fi mai puțin sigure cu privire la capacitățile militare ale SUA.

Prin acest exemplu dorim să susținem *nu* că un stat democratic ar trebui să își clasifice bugetul pentru apărare, ci că motivul pentru care nu face acest lucru este legat mai mult de aspecte politice interne (obligația democratică potrivit căreia cetățenii trebuie să știe cu ce se ocupă guvernul pentru a-și putea exercita drepturile și îndatoririle politice) decât de criterii abstracte de clasificare. Problema poate fi pusă în felul următor: aproape orice organizație – partid politic, companie, echipă de fotbal sau de alt tip – care se află în competiție cu alte organizații dorește să țină secrete majoritatea informațiilor cu privire la strategia sa de continuare a luptei, resursele disponibile și așa mai departe. În general, orice informație divulgată îi poate periclita poziția competitivă.

Acelaşi lucru este valabil şi în cazul activităţilor unui guvern privind securitatea naţională. Problema este reprezentată *întotdeauna* de găsirea unui echilibru între daunele care ar putea fi aduse la adresa securităţii naţionale şi imperativele unei ordini politice interne. Nu există nicio armonie între aceste două standarde, şi nu nici nu pot fi delimitate clar.

Presiunea pentru transparenţă nu vine întotdeauna din partea cetăţenilor. În ciuda tendinţei generale de păstrare a confidenţialităţii, orice guvern, dar mai ales unul democratic, consideră adesea utilă sau chiar necesară dezvăluirea unor informaţii pentru a-şi justifica acţiunile întreprinse şi a-şi atrage sprijinul cetăţenilor. După cum am observat anterior, pentru a justifica şi a-şi asigura sprijinul public cu privire la atacul cu bombă asupra Libiei din anul 1986, administraţia Reagan a dezvăluit informaţiile rezultate din decriptarea comunicaţiilor telegrafiate ale libienilor, potrivit cărora Libia era implicată în atacul terorist cu bombă de la o discotecă din Berlinul de Vest. Alertând guvernul libian cu privire la interceptarea comunicaţiilor, administraţia şi-a pus în pericol importante surse secrete.

Supraclasificare. Au fost aduse critici repetate la adresa guvernului SUA cu privire la clasificarea prea multor informaţii şi stabilirea unui nivel prea înalt de clasificare. Aceste critici au venit nu doar din partea comisiilor din Congres şi a analiştilor din serviciile secrete sau anumite administraţii, ci şi de la "cei din interior". De exemplu, comisia DoD din 1985 pe practici de securitate a observat că

> par să fie clasificate prea multe informaţii şi că acestea au un grad de clasificare mult mai ridicat decât ar trebui. Politica actuală prevede că semnatarul unui document clasificat este responsabil de clasificarea atribuită, însă, de cele mai multe ori, din necunoaştere sau din grabă, nu se acordă atenţia necesară acestor proceduri. Similar, deşi sunt permise contestaţii la adresa clasificărilor neadecvate, sunt puţini cei care îşi fac timp să discute pe marginea acestor clasificări cu cel care le-a făcut.[12]

Într-o oarecare măsură, după cum am observat deja, confidenţialitatea este o caracteristică normală a oricărui guvern. Dată fiind extraordinara deschidere a sistemului politic american, această practică pare anormală şi a ridicat mai multe obiecţii în Statele Unite decât în alte părţi. În ultimii ani, aceeaşi problemă a ieşit la iveală şi în alte state, în special în Marea Britanie, unde legile privind divulgarea informaţiilor guvernamentale sunt mult mai stricte decât în Statele Unite.[13]

În afară de principala daună – obstrucţionarea inutilă a accesului cetăţenilor la informaţii, reducând astfel abilitatea acestora de a înţelege şi de a face comentarii pe marginea politicii de securitate naţională – supraclasificarea ar mai putea avea şi dezavantajul scăderii credibilităţii sistemului de clasificare, ceea ce ar putea duce la o tendinţă de ignorare a

legilor, la nepăsare şi la "scurgeri de informaţii".[14] Dacă vor fi clasificate multe documente inofensive, importanţa interdicţiilor privind divulgarea neautorizată a informaţiilor clasificate se va reduce.

Este greu de spus dacă există o supraclasificare generală în guvernul SUA. Deşi orice sistem care gestionează milioane de documente în fiecare an poate produce rezultate nesigure, principala sursă de dezacord este reprezentată de existenţa unor puncte de vedere diferite referitoare la standardele care ar trebui aplicate atunci când se hotărăşte gradul de clasificare. Părerea celor care susţin faptul că supraclasificarea este exagerată este aceea că documentele sunt deseori clasificate pentru a-i scuti pe oficialii guvernamentali de complicaţii sau de critici. Aceste persoane susţin, cu alte cuvinte, că de fapt clasificarea îi scuteşte pe oficiali de justificarea acţiunilor întreprinse. Deşi acesta este un motiv inacceptabil în ceea ce priveşte clasificarea, de cele mai multe ori situaţia este mai complicată; criticile sunt îndreptate adesea nu doar către un oficial care a greşit faţă de public, ci şi către guvernul însuşi în raport cu puterile străine.[15]

După cum s-a menţionat la analiza acţiunilor secrete, secretizarea se impune de cele mai multe ori din motive diplomatice, şi nu operaţionale. Acest lucru este valabil şi pentru activităţile de politică externă în general. Cu toate acestea, ca şi în cazul acţiunilor secrete, guvernele au avut tendinţa, în ultimii ani, să fie mai deschise cu privire la multe aspecte ale politicii externe şi să fie mai puţin preocupate de detaliile diplomatice. Există o probabilitate mai mare în prezent decât înainte ca guvernele să recunoască derularea unor acţiuni de spionaj şi a altor operaţiuni secrete. În acest fel, guvernul nu mai poate fi criticat. Cu toate acestea, există posibilitatea ca motivele diplomatice să fie întemeiate. De exemplu, în 1977, *Washington Post* a susţinut că regele Hussein al Iordaniei ar fi primit unele subvenţii din partea CIA, afirmaţie ce nu putea decât să-i creeze acestuia unele dezavantaje în plan politic.[16] Păstrarea secretului unei astfel de relaţii pentru a evita criticile şi periclitarea poziţiei politice a unui şef de stat prietenos reprezintă un motiv întemeiat pentru secretizare, deşi, din punct de vedere operaţional, acest lucru nu este obligatoriu.

Subclasificare? Deşi se afirmă frecvent că guvernele au tendinţa firească de a supraclasifica, merită studiat dacă în anumite domenii nu se întâmplă exact opusul. Acest lucru poate fi valabil în cazul informaţiilor generate în afara guvernului, care sunt suficient de importante pentru securitatea naţională, iar astfel se justifică clasificarea şi controlarea lor. Cel mai concludent exemplu în acest sens sunt informaţiile legate de tehnologia armelor nucleare. Se presupune că aceste informaţii care ar ajuta la proliferarea armelor nucleare ar fi supuse unui control riguros, indiferent dacă provin din interiorul sau din afara guvernului.

În Statele Unite, această problemă a făcut obiectul Legii privind energia atomică din 1954, care a definit datele secrete ca fiind "toate informaţiile privind (1) proiectarea, fabricarea sau utilizarea de arme nucleare; (2) producţia de materiale nucleare speciale; sau (3) utilizarea unor

materiale nucleare speciale pentru producerea de energie."[17] Conform prevederilor legii, acest tip de informaţii sunt supuse controalelor indiferent dacă datele provin din interiorul sau din afara guvernului. (Aceeaşi lege interzice şi diseminarea de informaţii neclasificate privind proiectarea şi măsurile de securitate în cazul diverselor centre de producere sau utilizare a materialelor nucleare.)[18] Cu toate acestea, în Statele Unite există foarte multe informaţii despre materiale şi arme nucleare la dispoziţia publicului – de aici şi povestea conform căreia un absolvent de fizică strălucit, lucrând cu surse deschise la o bibliotecă publică, a realizat planurile pentru o bombă nucleară, pe care nişte experţi al căror nume nu a fost precizat le-au confirmat ca fiind viabile.

Printre alte informaţii care nu pot fi clasificate, dar care ar putea, în anumite situaţii, să beneficieze de protecţie, se numără:

- Informaţii financiare care ar putea facilita câştiguri ilicite pe pieţele de capital sau de mărfuri
- Informaţii tehnologice care nu trebuie dezvăluite inamicilor
- Informaţii personale care ar putea permite unui serviciu de informaţii advers să recruteze oficiali guvernamentali fie prin oferirea unor sume de bani celor cu probleme financiare, fie prin şantajarea lor.

Protejarea acestui gen de informaţii a implicat asigurarea securităţii comunicaţiilor, despre care vom discuta în continuare. Câteodată, însă, poate implica şi alte aspecte. De exemplu, în Statele Unite s-au făcut eforturi în vederea aplicării reglementărilor privind exportul de tehnologie şi în cazul diseminării lucrărilor ştiinţifice legate de aceste tehnologii; cu toate acestea, nu a fost elaborată nicio strategie practică în vederea realizării acestui lucru. În 1982, directorul adjunct al CIA, amiralul Bobby Ray Inman, a menţionat această problemă într-un discurs adresat Asociaţiei Americane pentru Progres Ştiinţific. Vorbind despre cercetarea criptologică teoretică şi aplicată, el şi-a manifestat îngrijorarea faţă de faptul că "publicarea la întâmplare a rezultatelor studiului respectiv va trezi interesul guvernelor şi entităţilor străine şi, prin aceasta, va produce daune ireversibile şi inutile intereselor de securitate naţională ale SUA." Dintre domeniile care ar putea aduce atingere securităţii naţionale prin punerea în circulaţie a informaţiilor tehnice, Inman a amintit "echipamentele şi programele informatice, alte tehnici şi mecanisme electronice, lasere, planurile agricole şi metodele de fabricaţie."[19]

În anii de după 1982, extinderea criptografiei publice a dat naştere unei controverse majore în Statele Unite cu privire la controlul programelor informatice care conţin algoritmi complicaţi de criptare. După cum s-a menţionat în capitolul 2, se fac din ce în ce mai multe studii criptologice în sectorul privat, datorită utilizării din ce în ce mai mult a comunicaţiilor electronice în scopuri comerciale. Deşi acest lucru aduce beneficii importante din punctul de vedere al securităţii naţionale (de exemplu, comunicaţiile criptate pot contracara încercările de furt tehnologic prin

"pătrunderea frauduloasă" în e-mailul sau în alte sisteme de comunicaţii ale unor companii), a generat îngrijorare cu privire la posibilitatea ca teroriştii, grupările de crimă organizată, de spălare de bani, etc. să obţină acces la funcţiile de decriptare, ceea ce va zădărnici eforturile de monitorizare a lor întreprinse de organele de aplicare a legii.

> În ciuda avantajelor recunoscute ale criptării, am susţinut de mult timp că proliferarea criptării indestructibile – având în vedere capacitatea sa de a împiedica total organele de aplicare a legii din ţara noastră să înţeleagă fişiere pe care s-a pus sechestru şi comunicaţii interceptate referitoare la acţiuni ilegale, care au fost criptate, iar apoi să poată acţiona prompt pentru a combate activităţile periculoase criminale, teroriste şi de spionaj şi a declanşa urmărirea penală – ar reprezenta o ameninţare serioasă şi radicală împotriva acestor interese centrale şi de o importanţă deosebită la adresa siguranţei publice.[20]

O modalitate propusă de reducere a acestui pericol a fost controlul exportului de software criptografic ce necesita algoritmi de criptare care depăşeau o anumită "putere" (măsurată în funcţie de dificultatea de rezolvare a cifrurilor rezultate).[21] În replică, producătorii americani de software au susţinut că acest tip de controale asupra exportului din SUA nu făceau decât să le permită competitorilor străini să pună mâna pe o cotă de piaţă şi mai mare, în detrimentul firmelor americane.

SECURITATE

Măsurile de securitate sunt demersuri întreprinse în scopul blocării capacităţii unui serviciu de informaţii inamic de a culege informaţii. Aceste măsuri au ca obiectiv împiedicarea unui serviciu de informaţii advers fie să acceseze, fie să exploateze orice acces pe care îl poate avea la personal, documente, comunicaţii sau operaţiuni în vederea obţinerii de informaţii importante; ele reprezintă zidul care protejează informaţiile clasificate. În această secţiune sunt analizate aspectele mai tradiţionale ale securităţii, care privesc protecţia împotriva eforturilor adversarului de a culege informaţii din surse umane; cele care se referă la posibilităţile sale de culegere din surse tehnice sunt analizate mai târziu sub denumirea de "activităţi contrainformative multidisciplinare".

Securitatea personalului

Securitatea personalului implică proceduri pentru verificarea potenţialilor angajaţi înainte de angajarea lor pe posturi care le oferă acces la informaţii pe care un serviciu de informaţii advers le-ar putea considera

interesante şi pentru garantarea faptului că actualii angajaţi continuă să îndeplinească standardele necesare pentru a avea acces la astfel de informaţii. Scopul principal al unei proceduri de verificare constă în evaluarea dorinţei şi capacităţii potenţialului angajat de a păstra secrete informaţiile clasificate. Elementele cheie ale acestei evaluări sunt caracterul şi loialitatea potenţialului angajat.[23] Evaluarea caracterului trebuie să ţină cont atât de stabilitatea mintală a individului, cât şi de posibilitatea ca, dintr-un motiv sau altul, acesta să fie vulnerabil la şantaj din partea unui serviciu de informaţii advers.

Investigaţii. În Statele Unite, procedurile de verificare stabilesc dacă un individ poate primi aviz de securitate – adică acces autorizat la informaţii clasificate. Investigaţia se bazează pe informaţiile furnizate de către individ într-un chestionar de securitate, fiind completată şi confirmată printr-o verificare la nivelul instituţiilor de stat (consultarea bazei de date a diverselor organe de aplicare a legii şi a altor agenţii guvernamentale), şi, în funcţie de importanţa informaţiilor la care va avea acces, se vor realiza interviuri cu prieteni şi cunoştinţe, foşti şi actuali vecini, colegi de serviciu şi de şcoală etc. În cazul informaţiilor de o importanţă deosebită, se impune efectuarea unei reverificări periodice pentru menţinerea accesului. Din mai multe motive, însă, poate că aceste verificări de *rutină nu sunt* foarte eficiente pentru a constata loialitatea şi caracterul personalului care va avea acces la informaţii clasificate.

Unele restricţii legale, care vor fi abordate în următorul capitol, împiedică FBI şi alte agenţii guvernamentale să obţină şi să păstreze o listă a membrilor aşa-numitelor organizaţii subversive, chiar dacă aceste organizaţii militează în mod deschis pentru înlăturarea violentă a guvernului SUA.[24] Un membru al unei astfel de organizaţii, care nu le-a spus cunoştinţelor despre apartenenţa sa la organizaţia respectivă şi nu a scris acest lucru pe formularele pentru avizul de securitate, are toate şansele să rămână nedescoperit.

În plus, schimbările sociale din Statele Unite au făcut şi mai dificilă obţinerea de răspunsuri sincere de la cunoştinţe, colegi, vecini şi alte persoane. În primul rând, există un resentiment tipic american faţă de verificările guvernului, ceea ce îi determină pe mulţi să nu fie dispuşi să transmită informaţii negative. Apoi, creşterea mobilităţii geografice a societăţii americane îngreunează şi mai mult localizarea fostelor cunoştinţe sau foştilor vecini, care oricum pot avea doar informaţii superficiale în ceea ce-l priveşte pe candidat. În anii 1990, cel puţin, climatul politic îi determina pe cei chestionaţi să nu ia foarte în serios întrebările despre loialitate şi activităţi subversive. Acelaşi lucru era valabil şi în ceea ce priveşte întrebările despre caracter şi stilul de viaţă. De exemplu, creşterea consumului de droguri în rândul clasei de mijloc (şi în special în rândul tinerilor) în ultimele decenii face dificilă stabilirea cazurilor în care folosirea acestora în trecut indică o adevărată problemă de personalitate şi o potenţială vulnerabilitate în faţa şantajului.

În cele din urmă, se pune problema dacă există posibilitatea de a-i asigura pe informatori că informațiile furnizate de ei vor rămâne confidențiale. Potrivit Legii privind confidențialitatea din 1974, persoanele au drepturi extinse de a accesa dosare guvernamentale cu informații despre ei înşişi; deşi există o excepție care permite unei instituții de anchetă să ascundă numele unui informator care solicită să rămână sub protecția anonimatului, este posibil ca acest lucru să nu le ofere o siguranță totală potențialilor informatori, care ar putea fi deranjați sau chiar mai rău dacă identitățile lor ar fi dezvăluite.

În primul rând, potențialii informatori ar putea fi îngrijorați de posibilitatea ca numele sau datele lor de identificare (cum ar fi numere de telefon) să fie dezvăluite întâmplător. În al doilea rând, chiar dacă identitățile lor nu sunt dezvăluite explicit, ei ar putea fi îngrijorați că cei care fac obiectul investigațiilor vor putea să le deducă din informațiile existente în dosarele guvernamentale. (Cu alte cuvinte, transmiterea unui detaliu aparent nesemnificativ – pe care, oricum, numai informatorul îl ştia – ar putea să-i dezvăluie identitatea. Este posibil ca ofițerul care revizuieşte datele înainte de a le transmite să nu-şi dea seama că acest detaliu poate să conducă la identitatea informatorului şi ca urmare, să-l transmită, fără să-şi dea seama de răul provocat). În fine, potrivit declarațiilor făcute în 1978 de către un oficial de la Departamentul de Justiție, Comisia Juridică a Senatului, "Teoretic, legile [privind Confidențialitatea şi Libera circulație a Informației] sunt suficiente pentru a ne proteja sursele, dar este cu totul irelevant dacă chiar reuşesc să facă lucrul acesta, atâta timp cât sursele noastre cred contrariul.[25]

O modalitate auxiliară de verificare a personalului este utilizarea poligrafului, cunoscut şi sub numele de detectorul de minciuni. Această tehnică a fost utilizată pentru prima dată de serviciile de informații din SUA; niciun alt serviciu de informații occidental sau ne-occidental nu are aşa de multă încredere în acest aparat. În SUA, CIA a pus foarte mult accent pe utilizarea poligrafului. Agenția a solicitat ca orice candidat să fie supus unui test cu poligraful şi ca tot personalul să fie obligatoriu supus periodic acestui test. Cu toate acestea, utilizarea poligrafului în cadrul guvernului SUA a fost combătută puternic de-a lungul anilor. Pe de altă parte, în urma arestării pentru spionaj a lui Geoffrey Prime, angajat al Centrului Guvernamental Britanic pentru Comunicații (GCHQ, agenția britanică de interceptare a comunicațiilor), oficialii americani i-au încurajat pe cei de la GCHQ să folosească şi ei metoda poligrafului. (Prime se pare că a compromis mai multe informații secrete provenind din surse tehnice, informații ce indicau o cooperare apropiată între Marea Britanie şi Statele Unite). Amenințarea implicită a recomandării de a folosi detectorul de minciuni era că SUA ar fi mai reținută în privința colaborării cu un serviciu secret care nu acceptă o astfel de procedură. Deşi se pare că utilizarea poligrafului are un puternic efect de intimidare şi în multe cazuri duce la dezvăluirea unor informații ascunse, acuratețea sa rămâne încă sub semnul întrebării.[26] Ca urmare a frecvenței cu care persoanele testate, deşi nevinovate, picau testul şi erau

respinse sau forţate să demisioneze, serviciile de informaţii străine au elaborat metode în vederea renunţării la acest procedeu de verificare.[27] Cea mai evidentă dovadă în acest sens este cazul lui Aldrich Ames, ofiţerul CIA care a spionat aproape nouă ani pentru Uniunea Sovietică şi Rusia, din aprilie 1985 până în februarie 1994. De două ori în această perioadă (1986 şi 1991) el a fost supus testului cu poligraful.[28]

Schimbarea tipului de ameninţare De la jumătatea anilor 1970, numeroase cazuri de spionaj au implicat angajaţi ai agenţiilor guvernamentale americane sau sub-contractori.[29] Motivaţia principală în aceste cazuri a fost cea financiară, sporită câteodată şi de o instabilitate emoţională.[30] Unul dintre cele mai complexe cazuri de acest tip este cel al lui Robert Philip Hanssen, agent FBI care a spionat pentru Uniunea Sovietică şi Rusia cel puţin din 1985 până la arestarea sa în 2001; mesajele sale către "manipulatori" sugerează o loialitate faţă de serviciile secrete sovietice/ruseşti care nu au nimic de a face cu ideologia.[31]

Aceste cazuri diferă în mod clar de faimoasele cazuri de spionaj americane şi britanice din anii 1940 şi 1950 (familia Rosenberg sau Kim Philby), unde motivaţia era în principal ideologică. Acest exemplu sugerează faptul că trebuie luate unele măsuri în vederea îmbunătăţirii securităţii personalului, precum realizarea unor profiluri psihologice detaliate sau crearea unui sistem de avertizare a cadrelor de conducere atunci când o persoană cu acces la informaţii clasificate fie se află într-o situaţie financiară dificilă, fie pare să aibă un stil de viaţă dincolo de posibilităţile sale financiare.

Securitatea fizică

Securitatea fizică se referă la metodele utilizate pentru a împiedica accesul fizic al agenţilor străini la informaţii clasificate. Se referă la securitatea locurilor în care sunt stocate informaţiile clasificate şi la caracteristicile sistemelor de alarmă pentru detectarea pătrunderilor neautorizate în zonele cu acces restricţionat şi, mai mult, sisteme sofisticate cu parole pentru protecţia informaţiilor clasificate stocate în calculatoare.[32] În mare parte, condiţiile de asigurare a securităţii fizice sunt cunoscute şi diferă foarte puţin, sau aproape deloc de măsurile pe care orice companie le întreprinde pentru a împiedica furturile de produse, echipamente sau informaţii şi documente interne de importanţă deosebită.

O diferenţă majoră este, totuşi, aceea că securitatea fizică are ca scop nu doar protejarea obiectelor materiale, cum ar fi documentele, care conţin informaţii ci şi a informaţiilor în sine. Acest lucru presupune controale mai severe privind accesul în zonele respective şi la echipamentele folosite acolo, având în vedere că un intrus ar putea implanta foarte uşor un dispozitiv de interceptare, iar serviciile de informaţii adverse ar avea astfel acces la zona restricţionată.[33] De aceea, este important ca tot ceea ce intră şi iese din acea zonă să fie supus controlului.

La fel, este foarte importantă existența unor dispozitive de "examinare" a zonei pentru a detecta orice dispozitiv de interceptare. Acest lucru atrage după sine dezvoltarea unor sisteme de interceptare a conversațiilor mai greu de detectat. Cel mai înalt nivel de tehnologie la care s-a ajuns în cadrul acestei spirale a ajuns în atenția publicului într-un şir de incidente în care a fost implicată ambasada SUA din Moscova. În anii 1970, de exemplu, o antenă sovietică a fost descoperită în şemineul cancelariei (clădirea ambasadei). Apoi, în anii 1980, s-a descoperit că un număr semnificativ de maşini de scris electrice aveau dispozitive de interceptare.[34] Mai târziu, a ieşit la iveală faptul că sovieticii compromiseră virtual întreaga structură a noii cancelarii pe care SUA o construiseră acolo. Sovieticilor li s-a permis să realizeze, fără a fi supravegheați de către americani, coloanele şi grinzile din beton prefabricat din care a fost construită cancelaria. Sovieticii au profitat de această eroare de securitate şi au proiectat un sistem de interceptare care utiliza întreaga structură ca antenă pentru interceptarea semnalelor şi transmiterea acestora. Sistemul a fost unul foarte sofisticat, iar Statele Unite nu au înțeles nici până acum cum funcționa.[35]

CONTRASPIONAJUL

Măsurile de securitate despre care am discutat sunt pasive, adică nu încearcă să contracareze acțiunile serviciului de informații advers ci urmăresc doar să împiedice accesului acestuia la informații. Măsurile mai active, care urmăresc înțelegerea modului în care acționează un serviciu secret concurent în vederea contracarării şi combaterii acțiunilor acestuia şi culegerii de informații în scopuri proprii, sunt cunoscute sub numele de contraspionaj.

Operațiunile de Supraveghere

O modalitate clară de a afla despre activitățile unui serviciu de informații advers este aceea de a iniția operațiuni de supraveghere asupra ofițerilor acestuia (monitorizarea permanentă) oriunde aceştia operează. O astfel de supraveghere încearcă să stabilească unde se deplasează ofițerii şi cu cine comunică sau cu cine intră în contact; aceste contacte pot fi utilizate ulterior pentru derularea unei anchete.

Deşi conceptul e simplu, în practică este vorba despre o activitate complexă. Abilitățile speciale ale ofițerului, despre care s-a discutat anterior din perspectiva culegerii de informații din surse umane, trebuie să servească înainte de toate contracarării acest tip de activitate. Ofițerul va fi instruit să evite propria monitorizare, şi va folosi tehnicile "predare fulger" şi căsuța poştală impersonală pentru a ascunde identitatea persoanelor cu care ia legătura. În plus, dacă observă filajul, ofițerul poate anula orice întâlnire planificată pentru a evita punerea în pericol a sursei sale. Este deci important ca operațiunile de supraveghere să fie mascate. Acest lucru este însă destul

de greu de realizat şi presupune un număr mare de persoane, având în vedere că ofițerul instruit în tehnici de contra-filaj va observa că aceeaşi persoană îl urmăreşte de o perioadă de timp.

Fiind o tehnică atât de complexă şi de costisitoare, este important ca aceasta să fie folosită într-adevăr asupra unor ofițeri de informații. Pozițiile care trebuie supravegheate, având în vedere că reprezintă funcții oficiale în care ofițerii serviciilor de informații activează în exterior sub acoperire sunt : diplomați, ofițeri consulari, reprezentanți comerciali, jurnalişti care lucrează pentru presa acreditată de guvern şi angajați ai organizațiilor internaționale, precum ONU, atunci când aceştia sunt selectați de către guvernele țărilor respective. Problema este aceea de a-i identifica pe cei care ocupă astfel de poziții şi care sunt cu adevărat ofițeri de informații.

Sunt mai multe feluri de a rezolva această problemă. În general, dacă un ofițer deține informații exacte despre modul de funcționare al unei anumite ambasade străine, de exemplu, atunci acesta poate spune care dintre oficiali îşi desfăşoară cu adevărat activitatea diplomatică sau consulară. Dacă unul dintre oficiali nu pare interesat de activitatea sa, atunci el poate fi implicat în culegerea de informații.

Se mai poate, de asemenea, ca observând tehnicile de rotație şi de înlocuire a personalului, să se poată stabili cine înlocuieşte pe cine; dacă X a fost identificat ca fiind ofițer de informații, atunci postul său va fi preluat, cel mai probabil, tot de un ofițer de informații. Aceleaşi tehnici folosite în general pentru culegerea de informații pot fi îndreptate şi către un serviciu de informații advers şi către agentul unui astfel de serviciu care acționează pe teritoriul altui stat. Cu cât se ştiu mai multe informații despre serviciul respectiv şi despre modul de funcționare, cu atât mai uşor va fi realizată operațiunea de filaj. În cele din urmă, agenții dubli, despre care vom discuta mai târziu în cadrul acestui capitol, pot stabili identitatea ofițerilor de informații străini.

Culegerea de informații

Cea mai bună modalitate de realizare a obiectivelor contraspionajului este aceea de a culege informații direct de la serviciul advers, prin mijloace umane sau tehnice. De exemplu, imediat după cel de-al doilea război mondial, agentul sovietic Kim Phliby, care lucra în cadrul MI6 (Serviciul britanic de informații externe) le-a furnizat agenților KGB informații prompte privind unele operațiuni secrete din statele baltice, Ucraina, Rusia şi Albania. Până în 1951, când Philby a fost forțat să demisioneze din MI6, acesta deconspirase, potrivit spuselor sale, sute de agenți britanici şi americani. În mod asemănător, serviciul de informații britanic beneficia pe la începutul anilor 1970, de sprijinul adjunctului şefului de misiune din Londra, Oleg Gordievski. Gordievski i-a asigurat pe britanici că KGB-ul nu avea niciun agent infiltrat în MI5 sau MI6 şi în 1983 i-a avertizat imediat asupra faptului că un ofițer MI5 care fusese dat afară se oferise să spioneze pentru KGB.[36]

Potrivit acestor exemple, activitatea de contrainformații nu este foarte diferită de activitatea culegere de informații în general, însă are ca țintă serviciul de informații advers şi nu guvernul, forțele armate sau alte instituții.

Defectorii şi Agenții Dubli

Ca şi în cazul celorlalte tipuri de culegere de informații HUMINT îndreptate către o societate închisă cum era fosta Uniune Sovietică, recrutarea şi dirijarea unui agent în interiorul unui serviciu de informații este o sarcină extrem de dificilă. Astfel, în trecut, Statele Unite şi alte state occidentale se bazau foarte mult pe defectori ai serviciilor de informații sovietice pentru contraspionaj. Vitali Yurcenko, directorul adjunct al departamentului de spionaj împotriva Statelor Unite şi Canada din cadrul KGB este un exemplu în acest sens. După ce a defectat în vara anului 1985, el a furnizat informații despre succesele spionajului sovietic împotriva Statelor Unite. De exemplu, cu toate că nu le cunoştea numele reale, în urma detaliilor personale şi operaționale pe care acestea le-a furnizat, Ronald Pelton, un fost angajat al Agenției Naționale de Securitate a fost arestat, iar Edward Lee Howard, un fost angajat CIA a fost pus sub acuzație.[37]

O altă metodă importantă de realizare a contraspionajului este prin intermediul agenților dubli. Ei sunt agenții care, deşi pretind că spionează pentru un serviciu advers, de fapt sunt controlați de către statul pe care se presupune că îl spionează. Este posibil ca ei să fi fost la origine spioni şi ca urmare a deconspirării lor să fie convertiți în agenți ai țării în care au fost prinşi. Sau mai pot fi "falşi defectori", agenți care se oferă să spioneze pentru un serviciu de informații inamic dar care de fapt rămân loiali țării lor. Între cele două categorii ar mai fi persoanele care, fiind abordate de către un serviciu de informații inamic, au raportat încercarea de recrutare autorităților şi au fost încurajați să intre în joc.

Aceste operațiuni care implică agenți dubli servesc aceloraşi scopuri contrainformative. La cel mai simplu nivel, ele permit unui serviciu de informații să înțeleagă metodele secrete ale adversarului şi să identifice ofițerii din serviciul de informații advers care sunt implicați în recrutarea de agenți. Ca urmare, operațiunea de supraveghere poate fi îndreptată către adevărații ofițeri de informații, acordând mai puțină atenție celorlalți oficiali care sunt într-adevăr diplomați, ataşați comerciali, etc.

Pe lângă identificarea ofițerilor de informații din serviciile adverse, aceste operațiuni îi ajută pe ofițerii de contrainformații să afle metodele operative utilizate de către adversarii lor. Folosind agenți dubli, poți afla cum procedează manipulatorii pentru a transmite instrucțiuni către sursă şi a primi informații de la aceasta, când şi unde preferă să se întâlnească, ce precauții îşi iau pentru a nu fi descoperiți, ş.a.m.d. Pe scurt, cunoscând modalitatea şi locul în care adversarul ia legătura cu sursele sale, ofițerii de contrainformații află despre abilitățile adversarului şi se poate proteja mai bine de acesta. Mai mult, cunoaşterea abilităților adversarului şi a tipului de

activitate al ofițerilor de informații contribuie la identificarea acestora de către serviciul contrainformativ. În cele din urmă, dacă un agent dublu este dotat cu echipament special, cum ar fi un transmițător radio, creat special pentru a fi utilizat de către agenți, atunci serviciul de informații respectiv are şansa de a-l studia. Acest lucru ar putea duce la interceptarea comunicațiilor radio între ofițerii de informații ai serviciului inamic şi adevăratele lor surse.

Din instrucțiunile pe care agenții le primesc de la manipulatori, un serviciu de informații poate afla care sunt informațiile prioritare pentru serviciul de informații advers. De asemenea, acest lucru mai poate oferi indicii valoroase cu privire la strategiile altor servicii de informații.

Una dintre cele mai interesante controverse din istoria serviciilor de informații are în prim plan instrucțiunile privind culegerea de informații date unui agent dublu britanic (nume de cod "Tricicletă") de către serviciul de informații german cu puțin timp înainte de intrarea Statelor Unite în cel de-al Doilea Război Mondial. Agentul, trimis în Statele Unite pe la jumătatea anului 1941, a avut la el un chestionar în care, printre altele, cerea informații detaliate cu privire la bazele americane din Hawaii. Informațiile oferite de către agentul dublu FBI-ului, respectiv lista întrebărilor şi posibila semnificație a fost ignorată total de către aceştia.[38] Oare dacă serviciul de informații american ar fi exploatat mai bine această informație, ar fi putut anticipa atacul trupelor japoneze de la Pearl Harbour?

Pe de altă parte, lipsa de interes într-un domeniu destul de important ar putea indica faptul că serviciul advers deține deja informații în acest sens; acest lucru ar putea reprezenta un indiciu important pentru activitatea de contrainformații.

În afară de obținerea unor informații despre serviciul advers, a modului de funcționare al acestuia şi a priorităților privind culegerea informațiilor, agenții dubli pot exercita un fel de control asupra acțiunilor întreprinse de serviciu. Simpla existență a unui agent dublu este suficientă până la un anumit punct; dacă serviciul advers ştie că are un agent cu acces la informații specifice, nu se mai deranjează să recruteze altul. Dacă agentul dublu reuşeşte să contracareze activitățile serviciului, atunci acesta poate proteja informații importante. În orice caz, dirijarea agentului dublu presupune mult timp şi efort din partea ofițerului de informații advers, reducând astfel resursele disponibile pentru recrutarea şi coordonarea agenților reali.

Mai mult, beneficiul pe care un agent dublu îl reprezintă în cadrul operațiunilor serviciului advers poate conduce la recrutarea cu succes a unui alt agent dublu, care poate avea acces la informațiile necesare serviciului advers. Primul agent dublu poate garanta pentru cel de-al doilea; de exemplu, primul agent ar putea confirma să zicem faptul că cel de-al doilea tocmai a fost avansat într-o funcție care îi conferă acces extins la informații deosebite sau că are probleme financiare şi are nevoie disperată de o altă sursă de venit.

Pentru a rămâne credibili, agenții dubli trebuie să fie capabili să ofere informații manipulatorilor lor. De cele mai multe ori, această problemă

se rezolvă cu aşa numitele informaţii "de umplutură" – aparent informaţii clasificate, de o importanţă deosebită care de fapt nu sunt aşa de importante. Alternativ, agentul dublu mai poate furniza şi informaţii reale şi importante pe care serviciul inamicul le-a obţinut deja pe alte căi. În astfel de cazuri, serviciul de informaţii care dirijează agentul trebuie să se gândească bine dacă păstrează credibilitatea acestuia, şi să contribuie la dublarea informaţiei transmise de agent, întărind astfel credibilitatea acestuia. Scopul este acela de a oferi cât de puţine informaţii utile fără a trezi suspiciunea serviciului de informaţii advers.

O altă modalitate mai ambiţioasă de a-i folosi pe agenţii dubli este aceea de a-i pune să furnizeze tot felul de informări şi dezinformări cu scopul de a induce în eroare serviciul advers. Până la un anumit punct, această modalitate controlează nu doar informaţiile culese de inamic, dar şi capacităţile analitice ale acestuia. Rezultatele pot fi extraordinare, deşi dificultăţile întâmpinate pot fi pe măsură.[39]

Dezinformarea este discutată pe larg în capitolele următoare. Această secţiune analizează două exemple de operaţiuni majore desfăşurate de agenţi dubli, foarte reuşite, una pe timp de război şi cealaltă pe timp de pace.

Agenţi Dubli din Timpul Războiului: Sistemul Încrucişat Una dintre cele mai cunoscute operaţiuni majore desfăşurate de agenţi dubli este Sistemul Încrucişat, prin care britanicii, aproape pe întreaga perioadă a celui de-al Doilea Război Mondial, "au dirijat şi controlat spionajul german din ţara lor".[40] După ce au prins un agent german la întoarcerea acestuia din Germania în Marea Britanie chiar la începutul războiului[41], britanicii au construit o reţea de presupuşi agenţi germani, lăsându-i pe germani să creadă în ei până la sfârşitul războiului.

Printre altele, agentul iniţial a furnizat informaţii în baza cărora germanii au emis acte de identitate false pentru a trimite alţi agenţi, care urmau să fie paraşutaţi sau transportaţi cu barca, facilitând astfel capturarea acestora de către britanici. În alte cazuri, noii agenţi trebuiau să-i contacteze pe cei care erau deja în activitate (controlaţi de către britanici) pentru bani sau alt fel de ajutor. Până la sfârşitul războiului, beneficiind de o anumită şansă, britanicii au reuşit să controleze întreaga reţea de spioni germani, interceptându-i pe cei noi la venirea acestora.

John Masterman, ofiţerul MI5 care a coordonat acţiunea, şi-a fixat şapte obiective:

- Controlarea reţelei de spioni a inamicului;
- Capturarea spioni noi infiltraţi în ţară;
- Identificarea persoanelor şi a metodelor folosite de către serviciul de informaţii german;
- Obţinerea de informaţii despre codurile şi cifrurile serviciului german;

- Obținerea de informații despre planurile şi intențiile inamicului prin chestionarea agenților acestuia;
- Influențarea planurilor inamicului prin răspunsurile trimise acestuia;
- Dezinformarea inamicului cu privire la planurile şi intențiile Marii Britanii.

Avantajele britanicilor au fost enorme. De exemplu, în 1940, agentul inițial a primit de la Berlin un cod pentru a comunica cu Germania. Deoarece acest cod s-a dovedit a sta "la baza mai multor coduri folosite de Abwehr [serviciul de informații militar german]," faptul că Britanicii au intrat în posesia lui "i-a ajutat să stăpânească în întregime şi de timpuriu sistemul [codului Abwehr]". Atunci când războiul a avansat, iar Britanicii au devenit mai siguri pe Sistemul Încrucişat, ei şi-au îndeplinit şi ultimele două obiective menite să îi inducă în eroare pe nemți. Punctul culminant a fost în 1944, când agenții dubli au fost folosiți pentru a susține stratagema prin care nemții au fost convinşi că debarcarea din ziua Z va avea loc în Calais, şi nu în Normandia.[42]

Datorită acestui succes al criptologiei (Ultra), serviciile de informații britanice au putut studia reacția germanilor la informările şi dezinformările raportate de agenții dubli. Printre altele, au putut observa care dintre rapoarte erau înaintate către înalta conducere din Berlin şi dacă liderii aveau încredere în informațiile furnizate. Acest feedback a fost vital pentru atingerea obiectivului de dezinformare, deoarece le-a permis britanicilor să scoată în evidență anumite elemente pe care nemții le trecuseră cu vederea, sau să modifice mesajele pentru a alunga orice umbră de îndoială din partea germanilor.

Controlarea rețelei de spionaj inamice a avut însă prețul ei: rețeaua trebuia să producă suficiente informații încât să satisfacă cerințele germanilor. În plus, informațiile pe care le producea nu puteau fi combătute prea uşor cu ajutorul informațiilor primite de germani pe alte canale de culegere a informațiilor, inclusiv de la potențiali spioni ce nu fuseseră capturați. (S-a dovedit că aceştia nu existau dar, desigur, britanicii nu puteau să îşi dea seama de acest lucru decât în timp; la început au fost nevoiți să presupună că ar putea exista alți agenți despre care nu ştiau.) Cu toate acestea, prețul plătit nu părea prea mare; din moment ce era posibil ca germanii să aibă o rețea de spionaj în Marea Britanie, era normal ca britanicii să o conducă.

Coordonatorul Sistemului Încrucişat considera mai târziu că poate el şi colegii săi au fost prea precauți, în sensul că britanicii au furnizat probabil mai multe informații reale decât era nevoie şi nu au folosit la maximum resursele de care beneficiau pentru a induce în eroare inamicul. Nu numai că germanii aveau mult mai puține canale auxiliare de informații decât credeau britanicii, prin care să verifice informațiile din Sistemul Încrucişat (aşa cum am spus mai sus, ei nu aveau niciun agent loial), dar aceştia au dovedit a avea extrem de multă încredere în agenții pe care îi considerau a fi în

serviciul lor. Acest grad ridicat de încredere este ilustrat şi prin eşuarea următorului plan:

> La un moment dat, unul dintre agenţi a fost dirijat [i s-a ordonat să se comporte într-un anume fel] pentru a arăta germanilor că este sub control, obiectivul fiind ca aceştia să îşi facă o idee falsă asupra metodelor noastre de a manipula un asemenea agent şi să îi convingă astfel că ceilalţi agenţi sunt loiali. Teoria s-a dovedit a fi una înţeleaptă iar gafele comise au fost imense şi flagrante, însă obiectivul nu a fost atins … Germanii credeau în continuare despre agent că este onest şi loial!

Agenţi dubli pe timp de pace: Operaţiuni cubaneze împotriva Statelor Unite. Pe 12 august 1987, *Washington Post* relata că un dezertor din serviciul cubanez de informaţii externe (DGI) ar fi declarat investigatorilor CIA că "un număr nedeterminat de oficiali din guvernul cubanez, pe care Statele Unite îi bănuiau de colaborare secretă cu CIA, ofereau agenţiei informaţii false sau nerelevante pregătite de DGI Cuba."[43] În urma acestei dezvăluiri, presa cubaneză a publicat relatări detaliate ale operaţiunilor acestor agenţi dubli, incluzând fotografii ale acestora în timp ce desfăşurau presupuse activităţi clandestine. Faptul că activităţile lor erau cunoscute de cubanezi până în cele mai mici detalii pare a confirma ipoteza că au fost agenţi dubli pentru cel puţin o parte din timpul, dacă nu chiar pe toată perioada, în care se presupune că spionau în Cuba. Conform unor surse cubaneze, unii dintre agenţi, conştienţi de faptul că Statele Unite cunoşteau adevărata apartenenţă, au trimis mesaje de rămas bun coordonatorilor lor din Statele Unite.

Fără a face o analiză atentă a informaţiilor furnizate de aceşti agenţi dubli, nu se poate stabili dacă în Cuba se desfăşura o campanie menită să inducă sistematic în eroare Statele Unite pentru a acţiona contrar intereselor proprii. Chiar şi în absenţa unui asemenea plan ambiţios, operaţiunea ar fi meritat din punctul de vedere al Cubei, deoarece ar fi necesitat efort şi timp din partea CIA, distrăgând astfel atenţia agenţiei de la informaţiile utile; de asemenea ar fi ieşit la iveală metodele operaţionale ale CIA, neutralizând astfel agenţii reali, dacă ar fi existat; şi nu în ultimul rând sistemul SUA de analiză a informaţiilor secrete ar fi fost asaltat de informaţii reale sau false menite să creeze confuzie şi să împiedice SUA să îşi formeze o imagine de ansamblu asupra evenimentelor din Cuba.[44]

ACTIVITĂŢI CONTRAINFORMATIVE MULTIDISCIPLINARE (MDCI)

Ce este MDCI?

Ameninţarea în materie de culegere de informaţii reprezentată de un adversar ce deţine tehnologie de ultimă oră nu se limitează la culegerea de informaţii din surse umane. În acelaşi fel, acţiunile contra-informative active nu se pot limita la contraspionaj. Din contră, ar trebui luat în considerare întreg arsenalul cu care adversarul ar putea culege informaţii din surse tehnice, cum ar fi fotografierea panoramică şi culegerea de informaţii din comunicaţii sau transmitere de semnale.

Astfel, principala sarcină a MDCI este de a evalua eficienţa resurselor adversarului pentru culegerea de informaţii din surse tehnice. Cunoaşterea acestor aspecte indică punctele vulnerabile ale informaţiilor, comunicaţiilor sau activităţilor şi ajută la găsirea celor mai bune modalităţi de protejare a acestora. Măsurile ce pot fi luate ar putea fi etichetate ca "măsuri tehnice" sau "de securitate", şi pot varia în funcţie de tehnologie. Cu toate acestea, perspectiva multidisciplinară este importantă deoarece ne încurajează să privim problema din punctul de vedere al adversarului – adică să luăm în considerare întreg spectrul de resurse de care acesta dispune.

Securitatea comunicaţiilor

Aşa cum interceptarea mesajelor, atât a celor scrise cât şi în format electronic, este una dintre cele mai importante metode de culegere a informaţiilor, protejarea conţinutului mesajelor este de multă vreme o sarcină a serviciului de contrainformaţii. Încă de la începutul secolului al douăzecilea, s-a pus accentul pe protejarea comunicaţiilor electronice transmise prin cablu sau unde radio.

Mesajele transmise prin cablu pot fi protejate fie prin prevenirea interceptării liniilor de transmisie a comunicaţiilor (citirea mesajului fie prin extragerea unei mici cantităţi de curent de pe linie sau prin interceptarea fluctuaţiilor câmpului magnetic din jurul liniei, cauzat de curentul ce trece prin acesta). Cablul din fibră optică este mai sigur, deoarece interceptarea mesajelor transmise pe această cale s-a dovedit a fi o problemă.[45] Semnalele radio, pe de altă parte, nu pot fi protejate în general; orice receptor de pe raza respectivă le poate intercepta. Unele semnale, cum ar fi transmisiunile prin microunde (folosite, printre altele, pentru apelurile telefonice la distanţă), sunt unidirecţionale (nu se dispersează în toate direcţiile, ci sunt concentrate într-o rază îndreptată spre destinatar), dar chiar şi acestea pot fi interceptate dacă receptorul este plasat în aria de acoperire a emiţătorului.

Conţinutul mesajelor radio era protejat la început prin criptare. Mesajele scrise pot fi criptate în mod tradiţional înainte de a fi transmise. În trecut, când se utiliza semnalul analog pentru transmiterea mesajelor de voce, se foloseau "telefoane sigure" sau "dispozitive de bruiaj"; acestea distorsionau semnalele voce într-o manieră complexă. Oricine ar intercepta un astfel de semnal primeşte un amestec de sunete fără sens, asemănătoare combinaţiei de litere dintr-un text cifrat. În principiu, reconstituirea textului original era la fel de dificilă. În prezent, atunci când mesajele voce sunt transmise în formă digitală, se aplică metode de criptare mai sofisticate.

Telefoanele sigure sunt relativ scumpe şi sunt folosite în principal pentru a transmite informaţii clasificate. Nu sunt des utilizate, ci se folosesc mai ales de către executiv. Astfel, majoritatea comunicaţiilor telefonice la distanţă, care folosesc transmisia prin microunde, fie printr-o reţea de turnuri (microunde terestre), fie între staţii la sol şi sateliţi, sunt vulnerabile la interceptare.

La mijlocul anilor 1980 în Statele Unite, această situaţie a captat atenţia publicului din cauza controversei privind locaţia noii ambasade Sovietice de la Washington. Construită în cartierul Mount Aldo, la înălţime faţă de centrul oraşului, ambasada şi clădirile adiacente erau poziţionate deasupra centrului oraşului Washington şi Virginiei de nord, inclusiv deasupra Casei Albe, Departamentului de Stat, Pentagonului şi majorităţii clădirilor guvernamentale. Se pot intercepta numeroase apeluri telefonice la distanţă din aceste clădiri şi din alte clădiri oficiale ale Rusiei din Statele Unite (consulate şi reprezentanţe comerciale din New York, Washington şi San Francisco; misiunile ONU din New York; facilităţile rezidenţiale şi de recreere din New York City, Long Island, New York şi pe ţărmul estic din Maryland).

Pe lângă faptul că oficialii guvernamentali folosesc telefoane nesigure, posibile ţinte ale culegerii de informaţii prin astfel de mijloace pot fi şi diverse companii de tehnologii avansate, comercianţi de bunuri care furnizează anumite produse pe care un stat le vinde sau cumpără în cantităţi mari (cereale, petrol şi aur), precum şi instituţii financiare. Un serviciu de informaţii ar putea de asemenea să vizeze indivizi ce au acces la informaţii clasificate pentru a afla detalii compromiţătoare din viaţa personală a acestora, cu scopul de a-i şantaja.

Au fost sugerate numeroase măsuri de prevenire pentru a reduce această vulnerabilitate. Spre exemplu, se poate regândi reţeaua de microunde pentru a elimina astfel riscul ca traseul să treacă pe lângă facilităţi de interceptare cunoscute sau potenţiale, folosindu-se cabluri subterane. Ca alternativă, se poate cripta semnalul transmis prin microunde prin bruierea semnalului atunci când se emite pentru prima dată şi decriptarea lui după ce a parcurs porţiunea respectivă de microunde. Ambele soluţii au hibe tehnice, iar implementarea lor presupune costuri destul de mari. Situaţia ar putea fi rezolvată prin folosirea fibrei optice, soluţie adoptată de companiile de comunicaţii din motive economice. Cablurile de fibră optică nu sunt mai puţin vulnerabile la interceptare, dar, datorită capacităţii mari (se pot transmite simultan mai multe semnale) au costuri mai mici decât cablurile de cupru tradiţionale sau decât reţelele de sol.

Securitatea emisiilor

Orice echipament electric emite unde electromagnetice; teoretic, prin interceptarea acestor unde este posibil să se deducă caracteristicile semnalelor electrice în urma cărora au fost emise. Astfel, prin prelucrarea acestor "unde" numite "emisii", se poate reconstitui textul unui document

tipărit pe o maşină de scris electrică sau transmis de la un computer către imprimantă. Se pot lua măsuri de securitate în acest sens prin protejarea echipamentului electric pentru reducerea intensităţii emisiilor, făcând dificilă interceptarea acestora.

Alte măsuri tehnice de securitate

Se pot lua anumite măsuri de protecţie împotriva altor forme de culegere de informaţii prin mijloace tehnice. În ceea ce priveşte supravegherea şi fotografierea prin satelit este posibil să se previzioneze orbitele acestora şi să se avertizeze obiectivele militare sau alte obiective de importanţă pentru ca acestea să înceteze activitatea şi să pună la adăpost echipamentele de importanţă deosebită, în locuri unde satelitul nu le poate fotografia; acest lucru este posibil în condiţiile în care s-ar putea stabili cu exactitate care dintre sateliţii adversarului sunt folosiţi pentru recunoaştere fotografică. Desigur, cu cât se ştie mai mult despre capacităţile sateliţilor, cu atât este mai uşor să se ia măsurile de prevenire necesare. Spre exemplu, după ce se determină punctele de pe suprafaţa terestră aflate exact sub orbita satelitului, este necesar să se cunoască la ce distanţă, în fiecare parte, obiectele sunt încă în raza camerei. Similar, culegerea de informaţii electronică sau prin telemetrie, poate fi prevenită prin criptare, bruiaj, schimbarea frecvenţei sau încetarea emisiei atunci când adversarul este în apropiere.

DEZINFORMARE ŞI CONTRA-DEZINFORMARE

Până acum, prin discuţia despre contra-informativ, am încercat să studiem diversele modalităţi prin care poate fi prevenită culegerea de informaţii de către adversar. Dacă acest lucru reuşeşte, adversarului îi vor lipsi probabil informaţiile necesare pentru a analiza situaţia în care se află, iar acţiunile sale, în orb, nu vor servi intereselor urmărite. După cum a rezultat din discuţia despre operaţiunile agenţilor dubli, în încercarea de a contracara operaţiunile de culegere de informaţii ale adversarilor este mai eficientă concentrarea asupra capacităţilor acestuia de a analiza informaţiile secrete – şi anume încercarea de a-l dezinforma.

Ce este dezinformarea?

Dezinformarea reprezintă încercarea de a conduce pe o pistă greşită analiza informaţiilor efectuată de adversar în ceea ce priveşte situaţia politică, militară sau economică. În consecinţă, formându-şi o imagine greşită asupra situaţiei, adversarul va acţiona în dezavantajul său. Aceasta este considerată o formă de acţiune contra-informativă deoarece urmăreşte să facă inutile operaţiunile de culegere de informaţii desfăşurate de adversar; în

plus, de cele mai multe ori sunt implicate metode contra-informative, cum ar fi operațiunile agenților dubli.

Dezinformarea este un concept asemănător cu eşecul unei acțiuni de culegere de informații. O acțiune de dezinformare reuşită înseamnă nereuşita operațiunii de culegere de informații desfăşurată de adversar. Există şi reversul, desigur; una dintre părți poate face greşeli importante în analiza informațiilor chiar şi fără dezinformarea venită din partea adversă. Cu toate acestea, în cazul nereuşitei acțiunii de culegere de informații, se poate identifica efortul părții adverse de a dezinforma. În ce măsură acest efort este responsabil pentru eşec, este o chestiune mai complicată.

Dezinformarea poate fi aplicată atât pe timp de pace, cât şi pe timp de război, deşi, din diverse motive, este de aşteptat ca dezinformarea să fie mai des utilizată pe timp de război.[46] Dezinformarea poate fi tactică sau strategică. Un exemplu de dezinformare o anumită țintă, în timp ce ținta vizată se află în altă parte. Exemplele de dezinformare strategică sunt mai puțin numeroase, dar extrem de importante, cum ar fi operațiunea de dezinformare din timpul celui de-al Doilea Război Mondial, prin care Aliații i-au indus în eroare pe germani cu privire la locația debarcării din Normandia.

Operațiunile de dezinformare pe timp de pace nu sunt extrem de des întâlnite, sunt mai puțin cunoscute şi uneori mai greu de depistat. Dintre cele mai spectaculoase astfel de operațiuni putem menționa ceea ce a fost cunoscut sub numele de "Încredere", o organizație sovietică ce se arăta ostilă noului regim comunist, dar care fusese, de fapt, înființată şi condusă din 1921 până în 1927 de predecesorul KGB, cunoscut sub numele de Cheka.[48] Folosindu-se de acest fals grup de opoziție, sovieticii au intrat în contact cu organizații anti-comuniste înființate de emigranți, precum şi cu serviciile de informații din Europa de Vest, reuşind astfel să prevină activitățile ostile pe care acestea le-ar fi putut demara; au convins presupuşi opozanți din Uniunea Sovietică să intre în contact cu organizația şi, astfel, Cheka le-a putut afla identitatea; de asemenea, organizația a răspândit în afara țării informații false privind situația din interiorul Uniunii Sovietice.[49]

În timpul anilor 1950 şi la începutul anilor 1960, Uniunea Sovietică a declanşat acțiuni de dezinformare menite să convingă Statele Unite că URSS deține mai multe resurse strategice nucleare decât avea, de fapt. După cum s-a menționat mai devreme, în timpul unui zbor demonstrativ cu ocazia unei ceremonii organizate în luna iulie 1955, sovieticii au "etalat" douăzeci şi opt de bombardiere Bizon – probabil mai multe decât existau în inventarul propriu – prin crearea condițiilor necesare, pentru ca primul grup de avioane să iasă din raza vizuală a spectatorilor (inclusiv a reprezentantului forțelor aeriene SUA) şi să revină pentru o a doua tură.[50] De asemenea, la finalul anilor 1950, liderii Sovietici, inspirați de prestigiul adus de succesul programului lor spațial, au furnizat informați exagerate cu privire la programul ICBM al URSS.[51] Astfel, sovieticii au contribuit la accentuarea temerilor SUA în ceea ce priveşte diferența uriaşă dintre bombardierele şi rachetele deținute de ei şi cele ale URSS (SUA se temeau că sovieticii aveau

să depăşească Statele Unite în ceea ce priveşte resursele nucleare strategice). Acţiunea de dezinformare a URSS părea menită să convingă occidentul să facă anumite concesii politice (de exemplu, în ceea ce priveşte statutul Berlinului) pe care, în mod normal, nu ar fi fost suficient de motivaţi să le facă.[52]

Conţinutul dezinformării – imaginea falsă pe care cineva doreşte să o creeze în ochii adversarului – depinde, desigur, de situaţie şi de reacţiile aşteptate din partea adversarului. Pe timp de război, de exemplu, una dintre părţi ar putea dori să lanseze un atac surpriză asupra inamicului şi, în acest caz, dezinformarea ar fi fost menită să îl convingă pe acesta că nu există iminenţa unui atac. În alte cazuri, cum ar fi debarcarea din Normandia, inamicul se aştepta să fie atacat, neexistând posibilitatea de a fi convins de contrariu. În acest caz, dezinformarea are scopul de a convinge inamicul că atacul va avea loc într-un alt moment, loc sau mod decât cele planificate.

Pe timp de pace scopul dezinformării este mai puţin evident. Un stat ar putea dori să îşi convingă adversarul că este mai puternic decât în realitate, sau să îl convingă să facă anumite concesii politice pe care altfel nu ar fi dispus să le facă. Sau, dimpotrivă, este posibil ca una dintre părţi să încerce să îşi disimuleze adevărata capacitate militară pentru a-şi linişti adversarul şi a-l determina să nu încerce la rândul său să îşi suplimenteze forţele militare. Dacă forţele militare ale unui stat sunt limitate de un tratat privind controlul armelor, acesta ar putea urmări ascunderea încălcării tratatului, obligând cealaltă parte să continue limitarea forţelor proprii.

Condiţiile necesare pentru reuşita unei acţiuni de dezinformare

Blocarea semnalelor reale şi fabricarea unora false. Dacă ne imaginăm procesul de culegere de informaţii ca fiind receptarea şi interpretarea semnalelor emise de activităţile părţii supravegheate, atunci putem spune că operaţiunea de dezinformare implică, în măsura posibilului, blocarea semnalelor reale (cele care reflectă activităţile reale) şi înlocuirea acestora cu unele menite să inducă în eroare. Putem oferi un exemplu simplu: rezervorul din locaţia X este camuflat, iar în locaţia Y se află la vedere un rezervor fals din material prefabricat. Dacă un avion de recunoaştere inamic survolează zona, ar putea trece cu vederea rezervorul din punctul X (deoarece semnalul vizual este blocat de camuflaj) şi va raporta rezervorul din punctul Y (cu condiţia ca semnalul emis de replica din prefabricat să fie asemănător cu unul real). În cazul operaţiunilor cu agenţi dubli, documentele reale, de exemplu, vor rămâne în seiful guvernului iar cele false, concepute special pentru operaţiunea de dezinformare, vor fi livrate recrutorilor de agenţii dubli.

Prima parte a misiunii o reprezintă problemele legate de securitate. Dacă se transmit prea multe semnale reale, este posibil ca adversarul să nu mai fie indus în eroare, cu toate că amestecul de semnale false şi reale l-ar putea înşela, împiedicându-l astfel să îşi formeze o imagine exactă asupra situaţiei. De aceea, una dintre cele mai importante condiţii pentru o acţiune

de dezinformare reuşită este abilitatea de a bloca cele mai multe, dacă nu chiar toate, canalele prin care adversarul ar putea culege informaţii. În general, acest lucru este mai uşor de realizat pe timp de război decât pe timp de pace, iar acesta este unul dintre motivele pentru care acţiunile de dezinformare au mai multe şanse de reuşită în primul caz.

Pentru blocarea canalelor de culegere a informaţiilor este nevoie, printre altele, de cunoaşterea în detaliu a canalelor prin care adversarul primeşte semnale. Este nevoie de resurse redutabile de contraspionaj, deoarece o sursă umană bine plasată ar putea dezvălui situaţia reală sau chiar planul de dezinformare. În plus, este nevoie de o bună cunoaştere a resurselor de culegere a informaţiilor prin mijloace tehnice pe care le deţine adversarul. Astfel, navele şi aparatele de zbor pot întrerupe orice tip de comunicaţii (de fapt, pot adopta "controlul emisiilor" sau "emcon", deoarece emisiile radar sau alte emisii electronice ar putea dezvălui poziţia vehiculului la fel de rapid ca şi transmisiunile radio) pentru a evita să fie detectate de sistemele de interceptare inamice. Acelaşi efect ar putea fi obţinut şi în cazul forţelor terestre, dacă acestea s-ar folosi de linii de sol (comunicaţii prin telefon sau telegraf, cabluri optice, etc.) în loc de unde radio, aşa cum au procedat germanii înaintea ofensivei din Ardeni din decembrie 1944. De asemenea, dacă se cunosc orbitele sateliţilor de recunoaştere ai adversarilor, activităţile pot fi oprite şi echipamentul camuflat sau mutat în locaţii acoperite, în momentul în care satelitul se află deasupra acestora, având posibilitatea de a le fotografia.

O a doua componentă a misiunii, fabricarea de semnale false, se planifică tot ţinând cont de resursele deţinute de adversar pentru culegerea de informaţii prin mijloace tehnice. Agenţii dubli pot transmite orice documente sau rapoarte false, atâta timp cât pot justifica modalitatea în care au avut acces la acestea. Dezinformarea sistemelor tehnice de culegere a informaţiilor este mai complicată, dar posibilă. Pentru a surprinde inamicul la Pearl Harbor, japonezii nu s-au limitat la a impune flotei de atac încetarea comunicaţiilor pe perioada traversării Pacificului. În plus, alţi operatori navali de radio s-au preocupat de transmiterea de mesaje false unul către celălalt, folosind semnalele flotei, dar cu transmiţătoare din Japonia. Astfel, dacă ar fi fost interceptate semnalele radio (deşi se pare că nu au fost) şi transmiţătoarele localizate, Statele Unite ar fi ajuns la concluzia că avioanele japoneze desfăşurau zboruri de exerciţiu în apele teritoriale. [53] În acelaşi mod, recunoaşterea fotografică poate fi păcălită, folosind replici ale armelor sau vehiculelor; pentru a afla cât de fidele trebuie să fie aceste copii, pentru a putea fi confundate cu cele reale, trebuie cunoscute capacităţile fotografice ale adversarului. [54]

Importanţa cunoaşterii resurselor pe care le deţine inamicul pentru a culege informaţii (canalele prin care îi parvine informaţia) este ilustrată de eşuarea planului britanic în timpul celui de-al Doilea Război Mondial. În primele luni ale războiului, marina britanică a echipat trei nave comerciale cu arme false, pentru a le face să semene cu nave de luptă şi un portavion. Obiectivul era deturnarea atacurilor germane dinspre flota principală

ancorată în portul Scapa Flow şi, în general, crearea confuziei printre germani cu privire la capacitatea reală a Marinei Regale. Cu toate acestea, istoria oficială a Serviciului britanic de contrainformaţii din timpul războiului arăta:

> Din păcate, în această etapă a războiului nu exista altă metodă de a informa germanii asupra existenţei navelor decât prin expunerea acestora în faţa avioanelor de recunoaştere; iar Forţele Aeriene Germane nu păreau să le fi reperat. Nevoia de a sincroniza mai multe canale de dezinformare nu era încă suficient luată în considerare.[55]

Feedback. În desfăşurarea unei operaţiuni de dezinformare apar numeroase incertitudini:

- Au fost blocate toate semnalele reale?
- Semnalele fabricate au ajuns la adversar?
- Acesta a tras concluziile dorite?

Pentru a obţine răspunsuri la aceste întrebări, se pot folosi mai multe metode pentru a afla modul în care adversarul evaluează situaţia. Dacă nu este suficient de alert ca să observe semnalele false, sau dacă nu le-a interpretat aşa cum ar fi dorit dezinformatorul, se pot fabrica alte semnale pentru a-i atrage atenţia şi a-l conduce spre interpretarea dorită. Dacă începe să simtă că ceva este în neregulă cu imaginea (falsă) a situaţiei pe care dezinformatorul i-a sugerat-o, se pot crea noi semnale pentru a alunga orice urmă de îndoială. Dacă adversarul a primit suficiente semnale reale pentru a-l ajuta să îşi facă o idee corectă asupra situaţiei, este recomandabil să se abandoneze operaţiunea de dezinformare şi să se treacă la un alt plan.

Feedback-ul se poate obţine în mai multe feluri. În unele cazuri (cum ar fi dezinformarea pe timp de război, sau cea menită să susţină un atac surpriză), acţiunile adversarului (sau lipsa acestora) ar putea fi suficiente pentru a indica dacă operaţiunea de dezinformare a reuşit. Astfel, absenţa oricăror semne de sporire a activităţilor militare (care s-ar fi putut observa foarte uşor) în cadrul flotei americane aflată la baza din Hawaii în prima săptămână a lunii decembrie 1941 ar fi oferit Japonezilor toate informaţiile de care aveau nevoie. În alte cazuri, pentru un *feedback* eficient ar putea fi nevoie de culegerea de informaţii cu privire la atitudinea părţii adverse faţă de situaţia dată; în cazul Sistemului britanic Încrucişat din timpul celui de-al Doilea Război Mondial, acest *feedback* a fost produs de interceptările Ultra, care au oferit britanicilor acces la deliberările înaltului comandament german.

Cu cât este mai întinsă în timp şi mai minuţios planificată dezinformarea, cu atât este mai importantă obţinerea unui *feedback* eficient. Partea dezinformată va răspunde mai greu la astfel de dezinformări şi, de

aceea, trebuie să se găsească o altă cale de a afla dacă momeala a fost muşcată. În general, operaţiunile de dezinformare pe timp de pace necesită un feedback mai bun decât cele desfăşurate pe timp de război. Pe timp de război, este de aşteptat ca adversarul să acţioneze mai rapid, în funcţie de capacitatea sa de evaluarea a situaţiei de fapt, demonstrând astfel dacă a fost păcălit. Pe timp de pace, adversarul este mai puţin presat să întreprindă acţiuni care ar putea dezvălui modul în care a procesat întreaga situaţie.

Acesta este unul dintre cele mai importante motive pentru care operaţiunile de dezinformare sunt mai rar întâlnite pe timp de pace decât pe tip de război. În plus, pe timp de război, este de aşteptat ca victima unei operaţiuni de dezinformare să fie presată să reacţioneze rapid; astfel, are mai puţin timp pentru a analiza situaţia şi a compara semnalele primite pe diverse canale; de aceea, este de aşteptat ca acesta să fie mai uşor indus în eroare.

Dezinformarea şi auto-dezinformarea. O falsă percepţie asupra situaţiei care este de aşteptat din partea adversarului trebuie determinată de acţiunile pe care le aşteptăm din partea acestuia. Cu toate acestea, viziunea respectivă trebuie să pară plauzibilă; de fapt, este de aşteptat ca scenariul de dezinformare să aibă succes dacă se bazează pe ceea ce adversarul presupune deja. De exemplu, dezinformarea din ziua Z a funcţionat atât de bine şi datorită faptului că Hitler era deja convins că debarcarea aliaţilor va avea loc la Calais, pe cea mai îngustă porţiune a Canalului. Astfel, semnalele fabricate au avut numai rolul de a-i întări această convingere şi de a alunga orice urmă de îndoială ce ar fi putut surveni în urma eventualelor semnale reale ce s-ar fi putut scurge; aceasta este o misiune mai uşoară decât cea care presupune determinarea adversarului să adopte în întregime un scenariu de dezinformare. De aceea nu este de mirare că cele mai impresionante succese ale operaţiunilor de dezinformare implică elemente majore de auto-dezinformare.

Contra-dezinformarea

Din experienţă putem afirma că este extrem de dificil să prevenim orice încercare de dezinformare venită din partea adversarilor. Chiar în perioada în care foloseau Sistemul Încrucişat, britanicii erau înşelaţi în acelaşi mod de către germani cu privire la operaţiunile tip gherilă şi cele de culegere de informaţii desfăşurate în Olanda. Începând de la sfârşitul verii 1941, odată cu arestarea unui agent de informaţii olandez care lucra pentru MI6, nemţii au reuşit să îi prindă pe toţi ceilalţi agenţi britanici trimişi în Olanda de către Biroul de Operaţiuni Speciale (SOE, ale cărui misiuni includeau sabotajul şi susţinerea grupărilor de rezistenţă anti-germane).

După ce au descifrat sistemul codificat folosit de aceşti agenţi, germanii au trimis britanicilor mesaje ce păreau a veni din partea agenţilor, care de fapt fuseseră arestaţi. Unii dintre agenţii arestaţi au cooperat la pregătirea şi transmiterea mesajelor; în alte cazuri ei au fost înlocuiţi cu operatori radio germani. Printre altele, cu ajutorul acestor mesaje s-au făcut aranjamentele necesare pentru paraşutarea de provizii suplimentare şi agenţi,

care erau, de fapt, capturați imediat. Operațiunea, denumită de germani *Nordpol* (Polul Nord) şi *Englandspiel* (meciul împotriva Angliei), a continuat până în 1944 când doi dintre agenții capturați au evadat din lagărul în care erau închişi. În acel moment, imaginându-şi că vor fi oricum deconspirați, conducerea serviciului militar german de contrainformații a decis să încheie acțiunea cu un mesaj simplu către Londra, trimis cu inspirație pe data de 1 aprilie.[56]

Unul dintre incidentele din cadrul acestei operațiuni arată cât este de puternică rezistența psihologică a unei persoane în fața ideii că ar putea fi dezinformată. Atunci când agenții britanici din Olanda codificau mesajele ce urmau a fi transmise către Londra, trebuia să includă şi un "test de securitate" – o anume deviere (care ar fi părut o simplă greşeală întâmplătoare) de la sistemul de cifrare. Aceasta ar fi indicat celor care primeau mesajul că ei erau cine susțineau că sunt şi că acționau pe cont propriu şi nu sub influența germanilor. De exemplu, să presupunem că un agent a fost instruit să facă o "greşeală" la a cincisprezecea literă a fiecărui mesaj transmis. Dacă germanii ar fi obținut sistemul de cifrare fără să înțeleagă principiul testului de securitate, orice mesaje trimise ar fi fost tratate ca fiind false, din moment ce nu conțineau "eroarea" stabilită.

În acest incident este vorba despre un operator radio german care transmitea mesaje în sistemul codificat obținut de la un agent britanic capturat. Deoarece operatorii radio pot fi uşor identificați după maniera în care bat punctele şi liniile din codul Morse ("stilul de scriere" sau "pumnul"), primul mesaj explica faptul că în Olanda fusese recrutat un nou operator, deoarece celălalt agent îşi luxase încheietura. Acest mesaj nu conținea niciun test de securitate şi ar fi trebuit recunoscut de SOE ca fiind fals; de altfel, acesta era şi motivul pentru care testul de securitate fusese inventat. În schimb, ofițerul de personal din Londra, deranjat de faptul că procedura nu a fost respectată şi evident, fără a ține cont de motivul pentru care procedura respectivă fusese instituită, a răspuns printr-un ordin ca noul operator radio "să fie instruit cum să folosească testul de securitate."[57]

În orice caz, primul pas spre evitarea dezinformării este să înțelegem cu funcționează aceasta; după înțelegerea factorilor care facilitează dezinformarea, putem cel puțin să prevedem posibilitatea de a fi dezinformați şi să recunoaştem câteva semnale de avertizare. O persoană este cu atât mai vulnerabilă în fața dezinformării dacă se bazează pe un număr mic de canale de informare şi dacă adversarul este la curent cu natura acestor canale şi modalitatea lor de operare.

De exemplu, folosirea excesivă a sateliților de recunoaştere fotografică, ale căror identitate şi orbite vor fi cunoscute mai devreme sau mai târziu de către cei fotografiați, creşte vulnerabilitatea în fața operațiunilor de dezinformare. Cunoscând momentele în care locațiile sale pot fi fotografiate, adversarul se poate asigura că anumite lucruri nu sunt observate: obiectele respective ar putea fi mutate în garaje sau hambare, ori acoperite cu echipament de camuflaj de fiecare dată când un satelit de recunoaştere trece pe deasupra zonei respective. De asemenea, adversarul

ştie când este momentul să expună echipamente false pentru a spori şansele ca acestea să fie observate şi confundate cu cele reale.

Situaţia este evident mai gravă (din punctul de vedere al potenţialei victime a operaţiunii de dezinformare) dacă adversarul poate afla din timp nu numai locaţiile ce pot fi fotografiate, ci şi care dintre acestea *vor fi* fotografiate. De asemenea, este şi mai grav dacă adversarul cunoaşte performanţele exacte ale satelitului. De exemplu, în cazul în care cunoaşte rezoluţia satelitului, va şti cât de fidelă trebuie să fie copia echipamentului pentru a părea identică. De aceea, sovieticii au dat o lovitură de maestru când au reuşit să intre în posesia manualului pentru satelitul american de recunoaştere fotografică KH-11. L-au cumpărat în schimbul a numai trei mii de dolari de la William Kamplies, după ce acesta a demisionat din poziţia de ofiţer inferior CIA în noiembrie 1977.[58] De aceea, fotografiile din satelit (care ar putea indica exact ce detalii pot fi identificate) sunt strict secrete. (Dacă este necesar ca fotografiile din satelit să fie făcute publice, calitatea acestora trebuie deteriorată pentru a nu dezvălui performanţele exacte ale sistemului).

Odată ce au fost înţelese riscurile implicate de folosirea unui singur canal de informare, se pot lua măsurile necesare. Cea mai bună soluţie ar fi extinderea operaţiunilor denumite şi "culegeri neaşteptate", adică fotografierea la ore şi în locuri pe care adversarul nu le poate anticipa. Desigur este mai greu de realizat acest lucru în cazul recunoaşterii prin satelit, din cauza faptului că orbitele sunt previzibile; operaţiunea se poate realiza mai uşor de-a lungul graniţelor sau coastelor teritoriului inamic, acolo unde este posibilă fotografierea aeriană.

Cu toate acestea, se pot urma anumiţi paşi chiar şi în cazul folosirii sateliţilor. Deşi adversarul ar putea avea capacitatea (prin studierea orbitelor, de exemplu) de a determina care sateliţi desfăşoară acţiuni de recunoaştere, acest lucru necesită timp şi va dura până va reuşi să transmită semnalul de alarmă în bazele sale militare. În primele ore de zbor ale satelitului sunt mai multe şanse ca fotografiile să fie făcute pe nepregătite. De aceea este bine să se stabilească cu atenţie ce locaţii vor fi fotografiate la prima trecere a satelitului. De asemenea se va acorda o atenţie deosebită modalităţilor prin care se poate prelungi perioada în care fotografiile se fac pe nepregătite, prin modificarea caracteristicilor de lansare şi deplasare ale sateliţilor, astfel încât adversarul să îi depisteze mai greu.[59] De asemenea, dacă s-ar găsi modalitatea prin care să se lanseze pe orbită mai mulţi sateliţi de recunoaştere în acelaşi timp (poate chiar şi falşi sateliţi pe care adversarul să nu îi poată deosebi de cei reali), este posibil ca adversarul să nu îşi mai poată proteja echipamentele şi acţiunile militare fără să îi fie serios afectate operaţiunile.

În schimb, mulţi susţinători ai culegerii de informaţii din comunicaţii o preferă pe aceasta faţă de celelalte metode de culegere de informaţii, deoarece mai mulţi factori garantează veridicitatea informaţiilor culese. Culegerea de informaţii din comunicaţii (COMINT) se poate face în cantităţi mult mai mari, crescând astfel şansele de a capta semnalele reale.

De asemenea, ar fi nevoie de un efort mult mai mare pentru a dezinforma COMINT printr-o rețea radio falsă (caz în care ar fi nevoie de folosirea de resurse şi personal pentru a fabrica semnalele), spre deosebire de cazurile în care ar fi nevoie să se expună echipamente false sau să se recruteze şi folosească un agent dublu.[60]

Este şi mai important faptul că adversarul nu va putea stabili cu exactitate ce canale de comunicații îi sunt interceptate; de aceea este posibil să trimită mesaje false care nu vor fi niciodată interceptate, în timp ce unele dintre cele reale ar putea fi. Însă nici această soluție nu este imbatabilă; spionajul (cum a fost cazul lui Geoffrey Prime, angajat la Agenției Naționale de Comunicații [GCHQ] echivalentul britanic al Agenției Naționale de Securitate [NSA] din SUA) şi anumite mijloace tehnice ar putea ajuta adversarul să identifice frecvențele sau liniile de comunicații pe care ceilalți le interceptează.[61] În acest caz, aceste canale de comunicații pot fi folosite pentru operațiuni de dezinformare.

O situație complicată de acest gen a avut loc în 1953-56 şi ilustrează dificultatea evaluării posibilelor operațiuni de dezinformare. Statele Unite şi Marea Britanie au săpat în Berlin un tunel din zona controlată de americani până în zona controlată de ruşi, pentru a instala dispozitive de interceptare pe mai multe linii telefonice şi telegrafice ce asigurau legătura între oraş şi comandamentul forțelor aeriene din Karlshorst. Tunelul a fost construit printr-un efort comun al MI6 şi CIA. Din nefericire, George Blake, ofițer superior al MI6 detaşat la Berlin, era de fapt spion sovietic. (A fost deconspirat în cele din urmă, arestat şi condamnat în 1961). Blake a participat la una dintre primele întâlniri la care s-au planificat chestiuni legate de tunel şi i-a informat pe ruşi.[62]

Oricum, cele mai importante comunicate telegrafice transmise de ruşi pe liniile interceptate erau codificate. Potrivit lui John Ranelagh, care, în relatările sale despre istoria CIA, pare a se baza pe numeroase informații de la foştii ofițeri, adevăratul secret al operațiunii era existența unei tehnici care permitea CIA să recupereze integral textul din mesajele criptate.[63] Britanicii nu ştiau despre această tehnică şi, de aceea, era imposibil ca Blake să fi dat detalii despre aceasta. Astfel, deşi fuseseră informați asupra dispozitivelor de interceptare, sovieticii ar fi putut continua să folosească linia telegrafică pentru mesajele importante, fiind convinşi că metodele de criptare garantau siguranța comunicațiilor.

Pe de altă parte, britanicii aveau rolul lor în culegerea informațiilor prin operațiunea tunelul din Berlin. Potrivit lui Ranelagh, "trebuia ca britanicii să efectueze analiza a jumătate dintre materialele rezultate".[64] Dacă acest lucru se întâmpla, ar fi fost evident că Statele Unite aveau o metodă de interpretare a mesajelor interceptate; dacă Blake ar fi aflat acest detaliu, Sovieticii ar fi realizat că tunelul reprezenta o problemă majoră.

Operațiunea tunelul s-a finalizat pe 21 aprilie 1956, la aproape un an după ce a fost interceptat primul mesaj, după ce se pare că ar fi fost descoperit de sovietici în timpul unor reparații la unul dintre cablurile pe care se montaseră dispozitive de interceptare. La momentul respectiv CIA,

neştiind despre existența unui spion sovietic în biroul MI6 din Berlin, a considerat descoperirea sovieticilor ca fiind accidentală. Acum, desigur, putem lua în considerare posibilitatea ca sovieticii să fi "făcut descoperirea" intenționat pentru a-l proteja pe Blake.

Este interesant de analizat în ce măsură "captura" din această operațiune poate fi privită ca dezinformare. Pe de o parte, este plauzibil ca sovieticii să fi aflat repede despre operațiune de la Blake; faptul că nu au intervenit ar putea sugera că se foloseau de situație pentru a dezinforma Statele Unite şi Marea Britanie. Pe de altă parte, sovieticii erau nevoiți să îşi protejeze sursa; dacă ar fi acționat imediat pentru închiderea tunelului sau pentru modificarea traseului comunicațiilor, ar fi riscat să alerteze Statele Unite şi Marea Britanie în legătură cu posibilitatea existenței unui trădător. De asemenea, dacă ar fi avertizat mai mulți ofițeri că liniile respective nu erau sigure, riscau ca Statele Unite şi Marea Britanie să afle şi să îşi dea seama că sovieticii ştiau despre tunel.

În orice caz, ar trebui analizate cu atenție informațiile rezultate în urma operațiunii; informațiile valoroase ar indica o probabilitate mai scăzută ca sovieticii să fi conştientizat faptul că linia nu era sigură (Ranelagh susține că primele indicii despre existența unui agent sovietic în cadrul MI6 ar fi fost obținute în urma operațiunii tunelul).[66]

Chiar şi în absența unor indicii conform cărora inamicul ar intercepta o anumită linie de comunicații, pentru dezinformare se putea crea o întreagă rețea de transmitere radio, cu unicul scop de a transmite mesaje care să fie interceptate de inamic; dacă rețeaua este suficient de mare, inamicul se va lovi de ea mai devreme sau mai târziu. Aceasta ar fi o măsură costisitoare şi complicată; însă pe timp de război este posibil de realizat. Înaintea debarcării din ziua Z, Statele Unite şi Marea Britanie au creat o asemenea rețea radio pentru a-i convinge pe germani că exista un grup armat al SUA, staționat în sud-estul Angliei şi pregătit să pornească "adevăratul" atac asupra zonei Calais. De fapt, grupul armat era format numai din câțiva soldați adevărați şi "comandantul" George S. Patton Jr.; cea mai mare parte a divizioanelor şi celorlalte componente existau numai pe hârtie şi în discuțiile radio purtate între operatorii rețelei false.

Acesta a fost un element important al operațiunii de dezinformare din ziua Z; operațiunea nu numai că a ajutat la conspirarea debarcării, ci i-a determinat pe germani să nu detaşeze trupe suplimentare în Normandia în zilele cruciale ce au urmat debarcării. Germanii au interpretat operațiunile din Normandia ca fiind o diversiune, o modalitate de a le distrage atenția de la invazia ce avea să urmeze. Conform unui studiu asupra operațiunilor de dezinformare din timpul Celui de-al Doilea Război Mondial:

> Rețelele folosite pentru comunicațiile radio false erau extrem de întinse şi complicate. La vârf se aflau 22 de formațiuni false [presupusele comandamente, precum şi armatele şi divizioanele componente]…

> Este aproape sigur că tocmai acest trafic radio simulat, din care cea mai mare parte s-a desfăşurat la distanţă mică de inamic şi care a fost uşor de monitorizat, a fost cel mai important factor al operaţiunii de dezinformare, cu excepţia agenţilor dubli.[67]

Aceiaşi factori ne pot ajuta să depistăm pericolul de a fi dezinformaţi prin culegerea de informaţii HUMINT. Atunci când culegerea de informaţii din surse umane se bazează excesiv pe dezertori creşte considerabil posibilitatea de dezinformare. În primul rând, spre deosebire de cazul în care există un agent infiltrat, inamicul cunoaşte identitatea dezertorului şi poate stabili cu aproximaţie la ce fel de informaţii a avut acesta acces. Inamicul nu poate împiedica dezertorul să spună ceea ce ştie, dar poate ţine cont de informaţiile respective într-o operaţiune de dezinformare. De aceea, informaţiile primite de la un dezertor sunt asemănătoare cu "culegerea anticipată".

În al doilea rând, adversarul poate infiltra cu uşurinţă un dezertor care să furnizeze informaţii false menite să dezinformeze. În cazul în care se folosesc excesiv dezertorii, inamicul ar putea pune la dispoziţie mai mulţi, ale căror rapoarte, deşi false, să se confirme între ele. Ca urmare a suspiciunilor că, încă de la începutul anilor 1960, Uniunea Sovietică ar fi procedat astfel faţă de Statele Unite, în 1970 au avut loc unele dintre cele mai grave conflicte interne din istoria CIA, între cei care luau această posibilitate în serios şi cei care o considerau deplasată. Aceştia din urmă au repurtat victoria în cele din urmă, când James Angleton, şeful biroului de contrainformaţii CIA şi cel mai fervent susţinător al primei viziuni, a fost concediat de William Colby în decembrie 1974.[68]

ANALIZA CONTRAINFORMATIVĂ

Aşa cum am demonstrat prin discuţia privind agenţii dubli şi dezinformarea, protecţia integrităţii operaţiunilor de culegere de informaţii este foarte greu de realizat şi implică mult mai multe elemente decât deconspirarea spionilor. De fapt, este posibil ca mai multe cazuri să fie legate între ele; pentru protejarea sistemului de culegere de informaţii împotriva infiltrărilor şi dezinformării este nevoie de un birou special de analiză contrainformativă care să joace rolul de memorie a instituţiei şi să analizeze toate aceste conexiuni.

Cea mai bună modalitate de a determina dacă sistemul de culegere a informaţiilor a fost penetrat este de a avea acces la o sursă la nivel înalt din serviciul advers (fie un agent în activitate, fie un defector). Chiar şi aşa, ar fi o chestiune de noroc dacă sursa respectivă ar putea identifica spionii după nume. Acest lucru ar fi posibil numai dacă sursa ar fi direct implicată în dirijarea lor, sau ar fi un ofiţer de rang foarte înalt din serviciul advers. Cel mai probabil sursa va putea oferi indicii privind identitatea spionilor. Pentru a obţine rezultate în urma acestor indicii, va fi nevoie de un efort analitic.

De exemplu, este posibil să se descopere că inamicul a avut acces la mai multe documente clasificate privind un anumit subiect. Presupunând că informaţiile au provenit de la un singur agent, se poate revizui lista de distribuire a documentelor compromise şi se poate stabili ce oficiali au avut acces la toate acestea. Este posibil şi ca sursa să ştie că spionul a avut o întâlnire cu coordonatorul său într-un anume oraş din străinătate, la o anumită dată. Informaţiile legate de călătorie pot indica ce oficiali, dintre cei care au acces la informaţii deosebite, au fost în oraşul respectiv la data aceea.

În plus, se pot folosi şi alte indicii care sugerează penetrări de orice fel ale sistemului. Astfel, dacă o operaţiune eşuează (un agent este descoperit sau un sistem tehnic de culegere a informaţiilor este compromis) într-un mod care sugerează faptul că adversarul avea cunoştinţă despre operaţiune înainte ca aceasta să aibă loc, trebuie investigate modalităţile prin care acesta a putut afla detaliile. Se vor descoperi fără îndoială multe canale prin care informaţia ar fi putut ajunge la inamic (indivizi cu acces la informaţii, sau vulnerabilităţi ori hibe de securitate). Dacă însă există o serie de astfel de eşecuri, se pot reduce pistele de investigaţie; spre exemplu, este posibil ca un singur individ să fi fost autorizat pentru a avea acces la toate informaţiile. Pe de altă parte, mai multe eşecuri consecutive pot indica şi faptul că a fost compromis un canal sau sistem de comunicaţii. De exemplu, de la sfârşitul anilor 1960 până la începutul anilor 1980, oficialii Marinei SUA au fost surprinşi să întâlnească de mai multe ori nave sovietice ce aşteptau navele de război americane în zone care fuseseră alese în secret ca spaţiu de exerciţiu. "Este ca şi cum ar fi avut o copie a Planurilor operaţiunilor", a declarat un amiral. Dar Statele Unite au aflat că documentele referitoare la cifrul naval au fost transmise în mod regulat Sovieticilor numai după ce a fost descoperită reţeaua de spionaj al lui John Walker în 1985 şi, deci, este posibil ca volumul mare al traficului de mesaje navale cifrate să fi fost citit de către aceştia.[69] În orice caz, o astfel de înlănţuire de evenimente ar trebui să alerteze un serviciu de informaţii privind posibilitatea ca adversarul său să aibă resurse umane sau tehnice eficiente pentru culegerea informaţiilor, care trebuie descoperite şi neutralizate.

Un caz asemănător este şi acela al trădării lui Aldridge Ames care a dus la pierderea unui număr important de surse de informaţii din Uniunea Sovietică în perioada 1985-1986 când CIA a fost alertată referitor la existenţa unei grave probleme.[70] La început, CIA a bănuit că i-au fost interceptate comunicaţiile de către KGB sau că anumite cazuri au fost prost coordonate (de exemplu, că expertiza nu a fost corespunzătoare, oferindu-le sovieticilor ocazia de a să le identifica) şi că "fiecare caz ar fi putut însemna "începutul sfârşitului" acestuia."[71]

Demersurile ulterioare ale CIA pentru a găsi cauza acestor pierderi au fost împiedicate de o sumă de factori: operaţiuni de dezinformare ale KGB, cazul Lonetree, şi suspiciuni conform cărora sovieticii au plantat microfoane în ambasada SUA din Moscova.[72] În cele din urmă, CIA şi-a îndreptat atenţia asupra lui Ames nu datorită analizei contrainformative în legătură cu pierderile suferite, ci datorită faptului că un coleg de al său a

observat şi a raportat că Ames ducea un stil de viață care depăşea mijloacele financiare de care acesta dispunea.[73]

CAPITOLUL 6

CONTROLUL PAZNICILOR: MANAGEMENTUL CULEGERII DE INFORMAȚII

Cele patru capitole anterioare au abordat tipurile de activități de culegere de informații şi unele aspecte referitoare la acestea. În continuare ne vom îndrepta atenția asupra relației dintre serviciile de informații şi autoritățile guvernamentale căreia i se subordonează precum şi asupra chestiunilor legate de managementul culegerii de informații din perspectiva superiorilor care nu fac parte din serviciile de informații, sau "a stăpânilor politici".

Din punct de vedere managerial (sau de administrație publică), informațiile prezintă două seturi de probleme importante. Primul set derivă din caracterul secret specific activității informative; acesta are în vedere dificultățile speciale legate de caracterul secret, pe care le întâmpină factorii politici cu responsabilități în supravegherea şi controlul activităților informative. Al doilea set derivă din incompatibilitatea dintre expertiză şi procesul de luare a deciziilor. Se referă la problemele privind atribuirea importanței cuvenite opiniilor experților (care susțin că posedă cunoştințe speciale) care se ocupă de consilierea factorilor de decizie (care au de fapt autoritatea de a lua decizii).

CARACTERUL SECRET ŞI CONTROLUL

Într-un guvern modern, cu mii de angajați implicați în structuri birocratice complexe, problema controlării numeroaselor activități ale acestora şi a verificării conformității acestora cu legea şi politicile adoptate de superiori este una foarte dificilă. În ceea ce priveşte agențiile de informații, problema principală constă în caracterul secret al activității acestora, oricât de legitimă ar fi necesitatea de a păstra secrete anumite surse de informare, metode şi activități dar şi în restricționarea accesului la aceste informații pentru un număr cât mai mic de oficiali din guvern.

Desigur că, în principiu, controlul activităților guvernamentale este organizat într-un mod ierarhic, astfel încât fiecare oficial este răspunzător în cele din urmă, prin lanțul de comandă, în fața şefului guvernului. Astfel, condiția minimă pentru control este aceea că fiecare superior are dreptul de a cunoaşte toate informațiile la care au acces subordonații săi. În general, această condiție este întrunită, deşi noțiunea de negare plauzibilă pune unele semne de întrebare importante în această privință.

Accesul teoretic la informații privind o anumită activitate nu este totuşi acelaşi lucru cu a avea suficiente cunoştințe pentru a o controla într-un

mod eficient. În alte domenii de activitate guvernamentală, controlul ierarhic direct, exercitat de către superiori este suplimentat prin alte mecanisme, atât oficiale cât şi neoficiale: inspecţii ale auditorilor sau ale inspectorilor generali, contestări şi plângeri referitoare la birocraţie, venite din partea unor părţi adverse, investigaţii efectuate de agenţiile de aplicare a legii, supraveghere legislativă, mediatizare şi reclamaţii sau altfel de reacţii ale publicului.

Aplicarea acestor mecanisme în activităţile informative necesită aducerea acestora la cunoştinţa unui număr mai larg de persoane care depăşeşte cercul de oficiali a căror necesitate de a fi informaţi derivă din implicarea concretă a acestora în astfel de activităţi. Cât de mare ar trebui să fie numărul de persoane informate depinde de mecanismele respective, întrucât unul dintre aceste mecanisme poate presupune informarea doar a câtorva oficiali din ramurile executive; un altul implică informarea membrilor organelor legislative şi a cabinetelor acestora; iar un al treilea, publicul general. În fiecare dintre cazuri, trebuie să se ajungă la un echilibru între riscul inerent lărgirii cercului celor cu acces la informaţii, pe de o parte, şi beneficiul care derivă din capacitatea mărită a superiorilor politici ai agenţiilor de informaţii de a controla activitatea acestora, pe de altă parte.

Negarea Plauzibilă

Întrucât toate mecanismele de control implică o mai mare diseminare a informaţiilor, se poate spune că, în general, există o tensiune între caracterul secret şi controlul eficient. Totuşi, în ceea ce priveşte activităţile informative, realizarea unui control eficient poate fi complicată şi mai mult de doctrina negării plauzibile, care sugerează că şi un control ierarhic fundamental al superiorilor poate fi pus la îndoială. Conform acestei doctrine, după cum am menţionat şi mai sus, activităţile informative care ar putea duce la complicaţii (datorită faptului că încalcă legislaţia internaţională sau din orice alt motiv) ar trebui să fie planificate şi executate astfel încât şeful guvernului să poată nega credibil că el sau ea ar fi avut vreo legătură cu acestea sau chiar că ar fi avut cunoştinţă despre faptul că acestea au avut loc. După cum am precizat, această doctrină este asociată de obicei cu acţiunile secrete, deşi se poate aplica şi altor activităţi informative, cum ar fi spionajul sau recunoaşterea fotografică aeriană care violează spaţiul aerian al ţintei.

Negarea plauzibilă poate complica controlul activităţilor informative cărora li se aplică. Pentru a fi eficientă, nu numai că necesită limitarea cunoaşterii activităţii la cel mai mic număr posibil de oficiali dar presupune şi absenţa unei proceduri oficiale de aprobare, dar şi a documentelor în care să se înregistreze respectiva aprobare. Activitatea însăşi ar trebui derulată astfel încât volumul evidenţelor să fie redus la minim, iar după finalizarea activităţii, probabil că ar trebui distruse orice documente create. Evident că astfel se creează condiţiile unor neînţelegeri şi a unei incertitudini cu privire la autorizarea unei anumite acţiuni. În special, fără o evidenţă scrisă, ar fi imposibil să se stabilească dacă o astfel de activitate a fost aprobată de către

şeful guvernului sau de un alt oficial de rang înalt care nu aparţine domeniului informaţiilor.

Toate acestea nu înseamnă că vreuna dintre agenţiile de informaţii este "un element ostil", ca să citãm o expresie atribuită senatorului Frank Church[1]. Cu condiţia ca situaţia să nu se schimbe, o agenţie de informaţii poate "sări gardul" mult mai uşor decât orice alte organizaţii guvernamentale. Împotriva acestei imixtiuni, pe de altă parte, trebuie precizat că agenţiile de informaţi investighează caracterul potenţialilor angajaţi mai atent decât o fac alte birouri guvernamentale şi că posibilitatea dobândirii unor avantaje materiale ilicite în cadrul unei agenţii de informaţii este mai mică decât în multe alte birouri guvernamentale, cum ar fi cele care se ocupă cu statistici şi norme economice, sau care fac afaceri în numele guvernului – de exemplu, prin atribuirea de contracte sau prin închirierea terenurilor aflate în proprietatea guvernului spre exploatare privată.

Poate că cel mai uimitor exemplu care ilustrează cum funcţionează, în practică, negarea plauzibilă a fost oferit de către investigaţia efectuată de Congres în 1975-1976 asupra activităţilor informative ale SUA. Un comitet senatorial, condus de către senatorul Church (cunoscut înainte sub denumirea de Comisia Specială a Senatului pentru studiul operaţiunilor guvernamentale referitoare la activităţile informative) a examinat tentativele CIA de a-l asasina pe liderul cubanez Fidel Castro la începutul anilor '60. Conform raportului comisiei privind implicarea CIA în planurile secrete de asasinare, "au fost insuficiente dovezi din care Comisia să poată trage concluzia că preşedinţii Eisenhower, Kennedy sau Johnson, consilierii apropiaţi ai acestora sau Grupul Special [grupul inter-agenţii care revizuia propunerile de acţiuni secrete] au autorizat asasinarea lui Castro."[2]

De fapt, dosarul găsit de comisie era uimitor de vag în ceea ce priveşte autorizarea. Oficialii importanţi ai CIA au declarat că ei s-au considerat autorizaţi în totalitate pentru a face ceea ce au făcut, dar că această autorizare nu a fost transmisă în atât de multe cuvinte, nici oral, nici în scris. Pe scurt, comisia a examinat cu atenţie documentele, sau mai precis lipsa acestora, la care te puteai aştepta într-o situaţie în care doctrina negării plauzibile era predominantă. Nimic din dosarul disponibil nu l-ar fi reţinut pe preşedintele John F. Kennedy sau pe fratele acestuia, Procurorul General Robert F. Kennedy (care a jucat un rol important în elaborarea strategiei politice faţă de Cuba), de la a nega în mod plauzibil orice implicare sau cunoştinţă despre tentativele de asasinat.[3]

Astfel, în ciuda unei dispute a priori privind dificultatea exercitării controlului asupra agenţiilor de informaţii, raportul Comisiei Church nu arată concret că acelaşi lucru s-a aplicat şi în privinţa tentativelor de a-l asasina pe Castro. Mai degrabă demonstrează cum ar funcţiona doctrina negării plauzibile pentru a proteja preşedintele de la a-şi asuma responsabilitatea. Astfel, inevitabil, rămâne valabilă posibilitatea că CIA ar fi scăpat de sub control, dar pare improbabil că chiar aşa a şi fost.[4]

Pentru cine lucrează serviciile de informații?

În orice caz, este ciudat ca un şef de guvern să îşi exercite atribuțiile de control în concordanță cu doctrina negării plauzibile. Nu se aseamănă deloc cu controlul obişnuit, pe care şeful guvernului îl exercită asupra departamentelor sau ministerelor prin lanțul de comandă oficial şi prin ordine scrise, hotărâri de guvern, declarații politice, memorandumuri şi aşa mai departe. Baza acestuia constă mai degrabă într-o loialitate directă sau personală a serviciului de informații față de şeful guvernului, decât într-o subordonare birocratică.

În trecut, serviciile de informații lucrau de obicei pentru un monarh, un ministru-şef sau un comandant suprem, în afara structurilor guvernamentale obişnuite. De exemplu, Sir Francis Walsingham, redutabilul secretar de stat al Reginei Elizabeth I a Angliei, a finanțat un serviciu de informații foarte eficient, în mare parte, din propriile fonduri (şi aproape a devenit falimentar din această cauză).[5] În mod asemănător, ducele de Marlborough, comandantul suprem britanic din timpul Războiului de Secesiune din Spania, a folosit o taxă de 2,5% pe salariile plătite de britanici pentru trupele străine din armata sa, ca şi alte câştiguri suplimentare (sau tradiționala mită, ca să folosim un limbaj mai puțin elegant), provenite din diverse contracte de achiziții, pentru a finanța un serviciu secret cu un aparent succes. El a considerat că aceste fonduri au fost cheltuite în mod adecvat pentru "a procura informații şi alte servicii secrete", dar ulterior a fost pus sub urmărire penală de către oponenții săi politici pentru deturnare de fonduri.[6] În ambele cazuri, distincția dintre fonduri sau activități publice şi private era una neclară. Evident că un astfel de aranjament nu poate fi tolerat foarte uşor de un stat birocratic modern, în care separarea între îndatoririle publice ale oficialilor şi interesele lor private se presupune că este absolută.[7]

Dar această problemă depăşeşte asigurarea răspunderii pentru fondurile publice. Problema şi mai importantă este cine poate autoriza pe oricine altcineva să se angajeze în astfel de activități. Acest aspect este foarte important într-o guvernare constituțională ca cea a Statelor Unite, în care puterea executivă este divizată între departamentele guvernamentale, iar demnitarii răspund în fața electoratului. Preşedintele îşi arogă dreptul de a autoriza derularea unor operațiuni informative, pe baza politicii sale externe şi a responsabilităților militare conferite de Constituție. În acelaşi timp, după cum am discutat în capitolul 4 referitor la acțiunile secrete, Congresul a insistat asupra unui circuit complet al documentelor care să facă legătura între activitățile informative şi cei care le-au autorizat. Astfel, un efect important al implicării Congresului în acest domeniu a fost subordonarea activităților informative controlului birocratic din cadrul ramurii executive.

Dar implicarea Congresului a depăşit şi problema autorizării şi controlării activităților informative de către ramura executivă. Comisiile de informații din Camera Reprezentanților şi Senat au subliniat cu succes dreptul de a fi "informate complet şi în mod regulat cu privire la activitățile

informative" şi de a primi "orice informaţie… cu privire la activităţile informative pe care le desfăşoară" oricare agenţie de informaţii.[8] Coroborat cu revigorata "putere a capitalului" (puterea Congresului de a-şi însuşi fonduri sau de a reţine fonduri pentru informaţii, ca şi pentru toate celelalte activităţi guvernamentale), Congresul putea folosi, şi într-o anumită măsură a şi folosit, aceste mijloace persuasive pentru a stabili o autoritate asupra informaţiilor, împreună cu preşedintele.

Rezultatul, după cum se exprima un fost director al CIA, Robert M. Gates,

> constă în faptul că astăzi CIA a ajuns într-o poziţie remarcabilă, echilibrată involuntar, aproape echidistant, între ramurile executive şi cele legislative. Administraţia ştie că CIA nu se află în poziţia de a tăinui informaţii faţă de Congres şi că este extrem de sensibilă la cererile Congresului; Congresul are o influenţă enormă şi multe informaţii dar, cu toate acestea, rămâne suspicios şi neîncrezător.[9]

Această discuţie privind implicarea Congresului în aspecte ce ţin de culegerea de informaţii ajută la explicarea unei alte probleme de control: astfel de controale nu vor da impresia organului legislativ că îşi exercită în mod eficient autoritatea asupra serviciului, oricât de oportun consideră şeful guvernului că este caracterul neoficial al controlului unui serviciu de informaţii. Din această cauză sunt necesare mai multe mijloace de control, cum ar fi cele deja menţionate (accesul oficial la informaţii, notificări privind anumite tipuri de activităţi, şi cerinţa ca fondurile pentru activităţile informative să fie alocate prin lege). Astfel, în Statele Unite, rezultatul implicării Congresului a fost că CIA, şi alte agenţii de informaţii, au fost subordonate controlului total al executivului şi aceluiaşi sistem de control parlamentar ca şi orice alt departament al guvernului. Chestiunea controlului parlamentar va fi abordată ulterior în acest capitol, în legătură cu discutarea relaţiei dintre serviciile de informaţii şi democraţie.

EXPERTIZĂ ŞI STRATEGIE

Secţiunea anterioară a făcut referire la relaţia dintre nevoia de a desfăşura activităţi în secret şi managementul activităţilor informative. Un alt set de probleme implică relaţia dificilă dintre expertiză şi strategie – adică, între cei care posedă cunoştinţe de specialitate referitoare la o problemă şi cei care sunt autorizaţi să stabilească şi să implementeze politica guvernului referitoare la aceasta. Această relaţie constituie o problemă în cadrul celorlalte departamente ale guvernului, indiferent de regiunile politice pe care le acoperă, fiind este o temă frecvent abordată de reprezentanţii administraţiei publice.

Multe probleme şi contradicţii apar de obicei între expertiză şi strategie. Importantă este problema rolului pe care expertiza îl poate avea în procesul luării deciziilor. Unde ar trebui trasă linia dintre funcţiile şi responsabilităţile experţilor, pe de o parte, şi cele ale factorilor de decizie, pe de altă parte? Evident că vrem ca strategia să fie construită pe baza celor mai bune informaţii disponibile; am condamna un factor de decizie care ar ignora faptele puse la dispoziţie şi şi-ar baza acţiunile pe propriile păreri nejustificate despre lume. În acelaşi timp, vrem ca strategia politica să fie stabilită de cei cărora sistemul politic (prin alegere sau numire) le-a acordat autoritatea de conducere; în orice caz, aceştia trebuie să-şi asume responsabilitatea pentru strategiile promovate, fără a ţine cont de informaţiile pe care s-au bazat acestea.

Ştiinţele sociale contemporane rezolvă teoretic această problemă prin intermediul distincţiei "fapt-valoare": ştiinţele sociale pot oferi fapte (inclusiv pronosticuri arbitrare, cum ar fi "dacă guvernul urmează politica X_1 va obţine rezultatul Y_1"), dar factorii de decizie deţin monopolul alegerii obiectivelor ce trebuie urmărite (dacă preferă rezultatul Y_1 rezultatului Y_2, sau vice versa).

Această soluţie teoretică oferă totuşi foarte puţine îndrumări practice. În primul rând, ştiinţele sociale sunt departe de a reuşi să facă pronosticuri arbitrare, în majoritatea domeniilor; desigur că, în ceea ce priveşte problemele de securitate naţională de care se ocupă serviciile de informaţii, acest tip de abilitate predictivă nu este disponibil. În al doilea rând, dezbaterile pe tema securităţii naţionale se ocupă mai mult cu diferite evaluări ale strategiilor aplicate, şi mai puţin cu dezacordurile referitoare la obiectivele care ar trebui urmărite. Cu toate că există un consens general asupra păcii, libertăţii şi prosperităţii ca obiective, nu acelaşi lucru se poate spune despre mijloacele necesare atingerii acestor obiective. Dimpotrivă, dacă se poate afirma cu oarecare certitudine că o strategie politică dată poate atinge aceste scopuri, rolul luării deciziilor s-ar diminua, sfârşind prin a dispărea.

Întrucât analiza informaţiilor poate oferi factorului de decizie indicii privind consecinţele adoptării unei strategii, distincţia teoretică faptă-valoare nu reuşeşte să identifice rolurile informaţiilor şi strategiilor. În practică, alegerile factorilor de decizie depind mai mult de părerile acestora legate de consecinţele strategiilor şi mai puţin de selectarea obiectivelor. (Într-adevăr, alegerea principalelor obiective este considerată atât de evidentă încât problema este rareori abordată.) Astfel, se pare că activitatea factorilor de decizie nu este atât de clar separată de activitatea experţilor (în acest caz, analiştii de informaţii şi cei care realizează estimări); deci, nu este surprinzător faptul că relaţia dintre serviciile de informaţii şi factorul politic este una destul de tensionată. Fiecare parte deseori priveşte acţiunile celeilalte părţi ca o violare a teritoriului său.[10]

"Uciderea Mesagerului"

Din perspectiva ofiţerilor de informaţii, disensiunile dintre serviciile de informaţii şi factorul politic par a se datora celui de al doilea. Dificultăţile

izvorăsc, conform acestora, din tendința factorilor de decizie de a nu acorda atenție raporturilor de informații care nu sprijină strategiile politice pe care aceştia doresc să le adopte, sau pe care le-au adoptat deja şi față de care şi-au luat un angajament. Ofițerii de informații deseori cred că factorii de decizie sunt interesați de produsele activității de informații numai în măsura în care acestea pot fi utilizate pentru a sprijini strategiile politice pe care le-au adoptat din motive complet diferite. Atunci când produsele activității de informații nu sprijină strategiile politice ale acestora, acestea sunt fie ignorate, fie se încearcă "ticluirea" acestora cu ajutorul presiunilor politice astfel încât să li se schimbe conținutul.

Această perspectivă a cristalizat opinia, care tinde să predomine atât în discuțiile academice cât şi în cele politice despre informații, că cea mai importantă caracteristică a oricărei organizații producătoare de informații este independența față de factorii de decizie. Numai o agenție de informații independentă poate rezista la presiunile politice pe care le-ar putea exercita factorii de decizie pentru a-şi pune de acord preferințele politice cu analizele acestora.

În contextul american, s-a oferit astfel cel mai important argument pentru existența unei agenții de informații *centrale* – care să nu fie asociată cu nici un departament guvernamental, cum ar fi Departamentul de Stat sau al Apărării – cu propriile capacități de culegere şi analiză a informațiilor. O astfel de organizație, conform argumentului, nu va fi predispusă la părtinirea care ar putea distorsiona produsul unui serviciu de informații care face parte din Departamentul de Stat sau al Apărării şi care este forțat să țină cont de preferințele politice ale organizației mamă sau de interesele bugetare ale acesteia.[11]

Această independență îi conferă dreptul agenției de informații de a se ghida numai după informații, fără să trebuiască să se preocupe de modalitatea în care produsul său va afecta procesul politic. După cum relatează un fost ofițer superior de informații american,

> Îmi aduc aminte că, la un moment dat, în calitatea mea de ofițer de informații pe spațiul Orientului Mijlociu, am fost invitat la Congres pentru a depune mărturie în cazul politicii americane (şi al puşcaşilor marini) din Liban, împreună cu un demnitar de rang înalt din cadrul Departamentului de Stat – numit politic. Pe drum, m-a avertizat că, atunci când voi răspunde la întrebări referitoare la şirul de evenimente din Liban, trebuie să mă limitez la discuții despre informații foarte actuale şi despre perspectivele pentru următoarele zile. Nu dorea nici o perspectivă cu bătaie lungă. Slavă Domnului că sistemul nostru mi-a permis să ripostez.[12]

Pe scurt, independența ar trebui să ajute la negarea aşa zisului sindrom de "ucidere a mesagerului", tendința de a da vina pe mesagerii (sau cel puțin de a-i ignora) – analiști de informații – care aduc veşti supărătoare, analize care nu sprijină strategiile politice favorite.

Percepția comună a acestui sindrom este aceea că acesta reflectă o anumită iraționalitate din partea factorilor politici; poate că cel mai bine este ilustrat de fragmentul din *Antoniu şi Cleopatra*, de Shakespeare. După ce l-a amenințat pe mesagerul care a informat-o că Antoniu s-a căsătorit cu Octavia, Cleopatra îşi explică comportamentul în următorul fel:

Deşi cinstit, nu e niciodată bine
Să aduci o veste rea.
Cu mii de guri
Solia bună să o vesteşti; cea proastă
'şi dă singură de ştire când o simți.

Ideea că nimeni nu ar trebui să fie avertizat în legătură cu evenimente neplăcute până când acestea nu au loc şi efect nu este o idee după care se poate ghida o agenție de informații. Orice factor de răspundere care adoptă o astfel de poziție ar acționa într-adevăr într-un mod irațional.

Cu toate acestea, un factor de decizie nu trebuie influențat de acest motiv irațional şi nu trebuie să îşi dorească să împiedice o agenție de informații să raporteze veşti nedorite. Într-un stat birocratic modern, nici un demnitar – nici chiar şeful guvernului – nu primeşte informații sau evaluări secrete referitoare la o anumită strategie politică pe care nu o primesc şi alți demnitari de rang înalt. Unii dintre ceilalți oficiali s-ar putea să nu fie partizanii politicii şi este de aşteptat ca aceştia să se folosească de informațiile negative în încercarea de a contesta sau de a profita de situația creată.

Această dificultate este exacerbată numai când informațiile sunt împărtăşite nu numai cu colegii demnitarilor şi rivalii birocratici ai acestora dar şi cu oponenții politici (de exemplu, partidul de opoziție din Congres). Din această perspectivă, nu este deloc irațional ca factorii de decizie să dorească să se asigure că informațiile oferă răspunsul "corect".

Desigur, ceea ce este în interesul oricărui factor de decizie nu trebuie să fie şi în interesul națiunii. Din punct de vedere național, ar trebui să căutăm ceea ce ar conduce la cea mai bună implementare a celor mai bune strategii politice. Din nefericire, aceste două scopuri pot avea cerințe contradictorii. În general, elaborarea celei mai bune strategii politice necesită ca toate produsele informative relevante să fie disponibile tuturor celor implicați. Mai mult ca sigur că informațiile şi analizele secrete vor sprijini argumente atât pro cât şi contra oricărei strategii politice propuse; toate aceste argumente ar trebui cântărite în luarea deciziei finale. Suprimarea accesului la informații sau opinii, sau ascunderea acestora față de anumiți participanți la procesul de luarea a deciziilor, va înclina balanța procesului şi va reduce posibilitatea obținerii celui mai bun rezultat.

Cu toate acestea, implementarea pune o problemă diferită; după ce se alege o strategie politică, argumentele aduse împotriva acesteia trebuie să fie ignorate în mare măsură. Încercările de a reargumenta problema de bază a strategiei politice de fiecare dată când trebuie luată o decizie tactică sau

încercarea de a reorienta strategia după fiecare informație nu poate duce decât la o strategie slabă, ambiguă, fluctuantă şi în cele din urmă ineficientă.[14]

Diseminarea la scară largă a produsului informativ, care conține părți ce contrazic presupunerile pe care s-a bazat strategia sau care se reflectă în mod negativ asupra progresului acesteia, îi poate părea demnitarului, care răspunde de implementarea strategiei, ca un rău inutil. În limbajul neaoş al preşedintelui Lyndon Johnson, problema este următoarea: "Luarea unor decizii este ca şi când ai mulge o vacă grasă. Vezi că iese lapte, apeşi şi mai tare şi laptele fierbe şi curge, şi exact atunci când se umple găleata, vaca o loveşte cu coada şi se varsă totul. Asta face CIA-ul cu procesul de luare a deciziilor."[15]

"**Informațiile imperiale**"

În timp ce analiştii de informații deseori cred că ataşamentul unui factor de decizie față de o strategie îl fac pe acesta sau aceasta să ignore sau să încerce să distorsioneze sau să şteargă informații relevante, factorii de decizie pot crede că deşi informațiile oferă deseori doar opinii frivole, aceştia ar trebui să considere aceste opinii ca literă de lege şi să ia decizii în consecință. În multe cazuri, nu este clar de ce opinia provenită din informații ar trebui considerată ca fiind mai autoritară sau obiectivă decât opinia altcuiva, inclusiv cea a factorului de decizie.

De exemplu, deseori o opinie bazată pe informații referitoare la probleme politice importante nu este bazată pe un nucleu sensibil de date concrete (de exemplu, raportul unui agent care activează în interiorul cabinetului sau al statului major al adversarului) ci pe datele care sunt disponibile şi factorului de decizie (sau unui jurnalist, de exemplu). În acest caz, factorul de decizie poate considera ca justificată decizia de a avea încredere mai degrabă în propria judecată decât în cea a unui analist anonim (necunoscut factorului de decizie); totuşi, criticii acestuia pot afirma că se comportă la fel de irațional şi ilegal ca şi Cleopatra. Ceea ce poate amplifica tensiunea este eşecul tipic al produsului informativ în a clarifica pe ce tip de probe se bazează. (Cu excepția demnitarilor de rang înalt, este posibil ca factorii de decizie să nu afle foarte multe informații despre sursele din spatele materialelor scrise pe care le primesc.). Factorul de decizie poate ajunge la concluzia că această lipsă de informații referitoare la surse presupune că principalele opinii provenite din informații sunt doar de natură speculativă, nefiind bazate pe date concrete.

În orice caz, probabilitatea ca factorul de decizie să aibă dreptate – ca judecata sa să fie superioară celei a analistului de informații – nu este neapărat una redusă. Este adevărat că, cel puțin în Statele Unite, comunitatea factorilor de decizie este uneori caracterizată de un mare procent de demnitari de rang înalt, dând naştere la un anumit grad de amatorism. Este posibil să fie vorba că, după cum spun cei din conducerea serviciilor de informații, "după câteva luni de activitate [noii analişti de informații] devin

unii dintre cei mai informaţi oameni din guvern, pe o anumită problematică… Pentru prima dată în viaţa lor, aceştia scriu pentru un public care ştie mai puţin decât ştiu ei."[16]

Cu toate acestea, nu este neapărat aşa, şi este posibil ca factorii de decizie care posedă expertiza necesară într-un anumit domeniu să desfiinţeze o notă cu informaţii care reflectă această perspectivă a abilităţilor lor. Mai mult decât atât, "factorul de decizie poate avea acces direct la informaţii care nu sunt disponibile analistului (conversaţii confidenţiale cu demnitari străini, de exemplu) şi, în orice caz, cunoaşte politica SUA mult mai bine decât analistul – aceasta deseori fiind cheia dezlegării misterului."[17] Astfel, în lipsa unei anumite informaţii secrete, sau a unei metode specializate de analiză, de multe ori opinia analistului de informaţii nu este îndreptăţită a fi acceptată în detrimentul opiniei altcuiva. După cum a subliniat Charles Fairbanks cu privire la o controversă asupra intenţiilor sovieticilor faţă de Iran în 1985 (existenţa unei ameninţări a sovieticilor asupra Iranului a constituit o problemă majoră care a afectat politica SUA în ceea ce priveşte această ţară),

> Iar în ceea ce priveşte mijloacele de analiză utilizate de către Comunitatea de Informaţii, nu există nici un secret în această privinţă: mijlocul este *analiza*, acelaşi tip de analiză ca cea folosită de un demnitar din afara Comunităţii de Informaţii sau a unui reporter sau a unui cetăţean în încercarea de a interpreta fapte asemănătoare. Elaborarea unei Estimări de Informaţii Naţionale Speciale (SNIE) pe o astfel de problematică… este de fapt acelaşi exerciţiu ca cel depus, în sensul bun sau prost, de unul dintre membri echipei [Consiliului Naţional de Securitate] atunci când au hotărât să vândă arme Iranului. Este un exerciţiu de raţionament politic.[18]

Numai atunci când rezultatul unui astfel de proces de raţionare primeşte eticheta de "informaţie" (şi o ştampilă cu caracterul documentului) se poate pretinde că este vorba de "un nucleu concret de fapte care transcende argumentele politice dubioase sau interesate ale altor agenţii şi care va servi ca test neutru de evaluare a acestora."[19]

Aceeaşi situaţie poate exista atunci când există "fapte concrete" disponibile analistului de informaţii, pentru că sunt rare situaţiile în care aceste fapte sunt înţelese de la sine. Acestea trebuie interpretate într-un anumit context iar acest context este furnizat, în primul rând, de către analist. Cu toate acestea, acest context se bazează pe raţionamentul speculativ în privinţa căruia este posibil ca analistul să nu aibă un avantaj special faţă de factorul de decizie. După cum sublinia Graham Fuller, un fost ofiţer de informaţii pe spaţiul Orientului Mijlociu,

> Pe măsură ce informaţiile devin mai generale, de natură strategică, creşte şi sensibilitatea interpretării acestora…. [De exemplu, întrebări de genul] cât vor rămâne la putere

> tiranii geriatrici de la Beijing? Dacă Saddam este înlăturat de la putere, se va scinda Irakul? Va reuşi Europa să menţină NATo? … [reprezintă] materiale pentru informaţii strategice. Este important ca analiştii să aibă datele dar, până la urmă, este nevoie de raţiune pentru a încerca să dea răspunsuri[,] … [iar astfel de raţionamente] vor apela la percepţia generală a individului despre 'cum funcţionează lumea' … o perspectivă coerentă asupra politicii internaţionale… Acest gen de înţelegere este ideologică prin natura sa… pentru că impune o ordine… într-un amalgam foarte difuz de date şi evenimente…. Nimic altceva nu poate învinge acest modern surplus de informaţii… Totuşi, lipsa unei astfel de construcţii este echivalentă cu apariţia unei imense superficialităţi a înţelegerii problemelor umane.[20]

Aceste argumente sunt contrare fluxului de opinii actuale despre acest subiect, care evidenţiază importanţa menţinerii independenţei serviciilor de informaţii faţă de politic şi a forţării politicului să le ia în considerare. Acordul dintre o strategie politică şi informaţiile secrete este deseori considerat ca o apreciere a raţionalităţii acesteia. Însă se pierde orice sens al solidităţii informaţiilor însele – se bazează pe un fapt incontestabil sau pe o speculaţie destul de contestabilă?

Acest punct de vedere poate fi luat în seamă şi în ceea ce priveşte circumstanţele apariţiei articolului lui Fairbanks din care am citat în pagina anterioară. Informaţii referitoare la elaborarea unei SNIE, la care face referire, - conform căreia posibilitatea ca sovieticii să invadeze Iranul era una relativ mică - au fost transmise presei pe cale neoficială, evident pentru a critica "vânzarea de arme Iranului în secret, pe care preşedintele Reagan a ordonat-o în ianuarie 1986 parţial pentru a sprijini Iranul împotriva 'intervenţiilor din partea Uniunii Sovietice.'" În articolul în care a apărut această scurgere de informaţii, se susţinea că "analiza pare a pune sub semnul întrebării o analiză primară raţională a Casei Albe".[21] Cu alte cuvinte, raţionamentul pe baza informaţiilor a fost utilizat ca piatră de temelie pentru o strategie politică, în ciuda "concreteţii" dovezilor pe care s-a bazat.

Acest tip de controversă are loc din cauza importanţei acordate "independenţei" serviciilor secrete din sistemul american. Prin comparaţie, sistemele de informaţii ale altor ţări (cum ar fi Marea Britanie) sunt mai puţin preocupate de protejarea "purităţii" raţionamentelor bazate pe informaţii şi mai interesate de a se asigura că expertiza proprie a factorilor de decizie poate contribui la procesul estimativ. După cum observă Loch Johnson,

> Produsul final american este o estimare *informativă*, în timp ce produsul final britanic este o evaluare mai generală care presupune o combinaţie între raţionamentul politic *şi* cel al

> ofiţerilor de informaţii… De fapt, cultura britanică încurajează combinarea [informaţiilor secrete cu strategia politică], în speranţa că cele mai bune decizii politice rezultă mai degrabă din schimbul de experienţă dintre specialiştii în afaceri internaţionale ai ţării.[22]

Independenţa serviciilor secrete

Date fiind potenţialele surse de fricţiune din relaţia servicii de informaţii şi factorul politic, problema privind gradul de independenţă al serviciilor secrete faţă de factorul politic este una foarte complicată. În cadrul structurilor militare, de exemplu, ofiţerul de informaţii de grad superior face parte din echipa comandantului în aceeaşi măsură (şi deci la fel de subordonat) ca şi orice alt locţiitor; nici nu se pune problema independenţei. Într-adevăr, nici măcar adevăratul sens al necesităţii ca o agenţie de informaţii să fie "independentă" nu este clar. În principiu, nimeni nu ar susţine independenţa unui serviciu de informaţii faţă de şeful guvernului. Cu toate acestea, după cum indică şi discuţiile de mai sus, se doreşte deseori ca informaţiile să fie utilizate drept criteriu neutru de arbitraj în cadrul disputelor politice – nu numai dintre oficialii din guvern dar şi dintre oficialii din guvern şi criticii legislativi şi extra guvernamentali ai acestora. Asta implică independenţa faţă de toate autorităţile guvernamentale şi o responsabilitate directă, corespunzătoare faţă de un alt grup, fie un corp legislativ (ca reprezentant al opiniei publice) sau chiar opinia publică.

După cum am discutat anterior, principalul argument pentru independenţă derivă din sindromul "uciderii mesagerului": serviciile de informaţii trebuie să fie independente dacă analiştii trebuie să fie capabili să spună adevărul aşa cum îl percep ei. În acest context, independenţa înseamnă capacitatea de a proteja analiştii individuali de presiunile sau ameninţările care i-ar putea determina să facă concluziile trase de ei mai acceptabile pentru beneficiarul produsului. Într-o oarecare măsură, acest gen de independenţă poate fi realizată prin crearea unei agenţii *centrale* de informaţii, una care se subordonează şefului guvernului dar nu beneficiarilor importanţi ai informaţiilor cum ar fi departamentul sau ministerul afacerilor externe sau al apărării naţionale. Cu toate acestea, înşişi şefii guvernelor sunt beneficiari ai informaţiilor cu toate că poate că au investit o mare parte din propria imagine într-o strategie politică. În acest caz, problema reapare la un nivel superior. Până la urmă, atâta timp cât serviciul de informaţii face parte din guvern, singura măsură de siguranţă este verticalitatea directorilor serviciilor de informaţii –disponibilitatea şi abilitatea acestora de a proteja analiştii de presiuni exterioare.

Independenţa este deosebit de importantă atunci când este nevoie să se abandoneze strategiile politice care nu dau rezultate sau pe care schimbarea circumstanţelor le-a învechit sau le-a făcut contraproductive. În acest scop, unele mecanisme trebuie să prezinte asigurări că toate informaţiile relevante, pozitive şi negative, sunt disponibile pentru revizuirea

strategiei politice. După cum sugerează citatul din Johnson, factorii de decizie trebuie să-şi canalizeze mare parte din energie implementării strategiilor politice, cu oarecare consecvenţă, în ciuda constantelor conflicte, îndoieli, atacuri politice – nu neapărat motivate de convingerea sinceră în superioritatea unei alte strategii politice – şi aşa mai departe. În aceste condiţii, este deosebit de dificil pentru astfel de oficiali să schimbe macazul şi să elaboreze o revizuire lipsită de prejudecăţi a strategiei politice.

În această situaţie, serviciile secrete au o poziţie de adversar întrucât evidenţierea domeniilor în care strategia politică nu dă rezultate sau a devenit inadecvată devine cea mai importantă funcţie a acestora. Cu alte cuvinte, acestea trebuie să contracareze presiunea politică exercitată asupra birocraţilor pentru a-i determina să fie buni coechipieri strategiile politice actuale. De aceea, serviciul de informaţii care prezintă p informare care sugerează că strategia politică este învechită sau că obiectivul acesteia este greşit trebuie să aibă destulă independenţă pentru a rezista la presiunea generată de o astfel de situaţie.

În trecut, o astfel de situaţie, care a atras atenţia publicului, s-a referit la rolul comunităţii de informaţii în a verifica respectarea acordurilor privind controlul armelor. Acuzaţia că una dintre părţile cosemnatare a încălcat acordul privind controlul armelor, ar pune sub semnul întrebării decizia încheierii acestui acord de la bun început, sau, oricum, decizia continuării aderării la acesta. Dorinţa de a păstra acordul (sau de a păstra sau îmbunătăţi în general relaţiile cu partea respectivă) a oferit un mobil puternic pentru a ignora sau a ascunde dovezile incomode. În orice caz, dificultatea întâmpinată în încercarea de a forţa partea respectivă să respecte acordul sau de a întreprinde orice măsură care vizează încălcarea acordului a fost şi rămâne un factor determinant pentru a nega existenţa acestuia.

În plus, un serviciu de informaţii trebuie să fie suficient de independent pentru a lua iniţiativa de a cerceta probleme sau zone ale lumii fără să fie nevoie să i se ordone acest lucru de către comunitatea de factori politici. Un serviciu de informaţii ar trebui să scaneze orizontul pentru a depista potenţiale probleme din zonele care nu atrag atenţia factorilor de decizie. Această funcţie de avertizare implică inevitabil înaintarea către factorii de decizie a unor informaţii pe care aceştia nu le-au cerut şi pe care nu le doresc în mod special, pentru că nu le cunosc valoarea.

Dar independenţa prezintă şi dezavantaje. Poate că cel mai mare dintre acestea este riscul ca munca de culegere de informaţii să devină sau să fie percepută ca irelevantă în cadrul procesului de adoptare a strategiilor politice. Această situaţie poate avea loc pentru că analistul de informaţii nu ştie ce probleme sunt considerate a fi mai importante de factorii de decizie sau ce opţiuni pot fi luate în considerare pentru rezolvarea acestora.

Această problemă poate fi cauzată de mai mult decât simpla distanţă organizaţională sau fizică faţă de factorii de decizie. Analiştii de informaţii deseori refuză să coopereze în ceea ce priveşte implementarea strategiilor politice pe care nu le susţin. Fostul director al CIA, Robert Gates a oferit un exemplu care să ilustreze această problemă:

> Atunci când secretarul de stat Alexander Haig a afirmat că sovieticii se află în spatele terorismului internaţional, iniţial, analiştii de informaţii nu şi-au propus să abordeze problema din toate punctele de vedere, ci mai degrabă să dovedească faptul că secretarul nu avea dreptate – pur şi simplu să dovedească că sovieticii nu orchestrează întregul terorism internaţional. Dar prin această abordare, ei înşişi au mers prea departe şi au eşuat iniţial să descrie vasta şi bine documentata susţinere indirectă a sovieticilor faţă de grupările teroriste şi sponsorii acestora.[23]

Cu alte cuvinte, o strategie de abordare a problemei terorismului internaţional care ar fi obligat Uniunea Sovietică să îşi reducă sprijinul (direct sau indirect) acordat grupărilor teroriste a fost zădărnicită de faptul că analiştii serviciilor secrete nu au fost dispuşi să coopereze, considerând că o astfel de implicare a Uniunii Sovietice nu constituia decât o parte nesemnificativă a problemei terorismului. Poate că această idee era fundamentată, dar aceasta nu înseamnă că strategia respectivă era incorectă; este posibil, de exemplu, ca politica SUA să nu fi fost în măsură să abordeze principalele cauze psihologice, sociologice sau chiar politice ale terorismului sau ca rezolvarea acestor probleme să fi intrat în conflict cu alte obiective de politică externă.

Dacă serviciile de informaţii se concentrează prea mult (deşi acest lucru este necesar) asupra adoptării unei poziţii adverse (de exemplu, în cazul implicării în revizuirea strategiilor adoptate), devine tot mai dificil ca acestea să sprijine implementarea efectivă a strategiilor. Asumarea unui rol de sprijin presupune ca serviciile de informaţii să-şi concentreze eforturile asupra identificării şi analizării informaţiilor relevante pentru implementarea strategiei. În exemplul de mai sus, aceasta ar fi însemnat descoperirea mecanismelor prin care o grupare teroristă internaţională a primit asistenţă financiară şi logistică de la susţinătorii ei. Pentru a sprijini implementarea strategiei, un serviciu de informaţii ar trebui să nu insiste asupra concepţiei sale – potrivit căreia sprijinul acordat de un stat nu constituie o cauză principală a terorismului internaţional – cu privire la motivele pentru care strategia este eronată.

Serviciile de informaţii şi "era informaţională"

Progresul rapid al tehnologiei în domeniul telecomunicaţiilor şi al prelucrării datelor – principalele tehnologii specifice aşa-numitei "ere informaţionale" – a provocat schimbări ample în modul în care organizaţiile utilizează informaţiile.[24] Un factor deosebit de important a fost explozia informaţiilor din surse deschise. Pe lângă utilizarea pe scară largă a Internetului, prăbuşirea comunismului sovietic a fost poate cea mai importantă cauză care a facilitat accesul la informaţiile din surse deschise: de

la Vladivostok la râul Elba (care marchează frontiera dintre fosta Germanie Occidentală şi cea Răsăriteană) dispăruse un întreg aparat menit să păstreze secrete chiar şi cele mai banale evenimente.

În general, procesul cunoscut sub denumirea de "globalizare" a intensificat circulaţia transfrontalieră a informaţiilor şi a creat multe canale noi de informaţii. Globalizarea este un concept greu de definit; probabil cea mai importantă manifestare a sa este reprezentată de intensificarea comerţului internaţional şi a diviziunii muncii, care s-a făcut simţită în majoritatea statelor lumii. Acest lucru a dus la creşterea numărului de deplasări şi la extinderea mijloacelor de informare din ţările dezvoltate în întreaga lume (de exemplu, difuzarea CNN şi a altor canale de ştiri în hotelurile din diferite regiuni ale lumii).

Chiar înaintea erei informaţionale, factorii de decizie aveau acces la multe informaţii provenite din alte surse decât cele tradiţionale. Schimbările apărute în mediul politic internaţional şi cele determinate de "revoluţia informaţională" sugerează că în viitor vor fi disponibile şi mai multe informaţii provenite din afara serviciilor secrete.

Deşi existenţa şi accesibilitatea tot mai mare a surselor de informaţii din afara canalelor tradiţionale prezintă avantaje importante pentru factorii de decizie, ele creează şi o serie de probleme, legate de:

- localizarea acestor surse;
- evaluarea credibilităţii lor;
- analizarea informaţiilor pe care le furnizează şi coroborarea acestora cu informaţiile obţinute de la serviciile de informaţii;
- păstrarea confidenţialităţii cu privire la aspectele de interes pentru factorii de decizie.

Deşi aceste probleme nu sunt noi, se pune întrebarea dacă schimbările aduse de era informaţională sunt de o asemenea amploare încât să impună abordarea lor într-o manieră mai sistematică decât până acum. Factorii de decizie au nevoie de "specialişti în informaţii" pentru a-i ajuta să selecteze anumite informaţii din multitudinea celor existente în era informaţională? În prezent, această funcţie este îndeplinită în trei modalităţi:

- De către factorii de decizie
- De către personalul subordonat acestora
- De către analiştii de informaţii

Fiecare dintre aceste modalităţi prezintă anumite avantaje şi dezavantaje. Desigur, factorii de decizie sunt responsabili pentru acţiunile lor şi, prin urmare, trebuie să se asigure că au primit şi înţeles corect informaţiile relevante. Astfel, cel puţin o parte a procesului de analiză le aparţine. De asemenea, aşa cum am menţionat deja, ei pot avea acces la surse de informaţii indisponibile pentru alţii: comunicaţii la nivel înalt cu alte guverne, precum şi intenţiile şi planurile unor oficiali din cadrul propriului

guvern şi ale unor factori neguvernamentali (cum ar fi anumiţi membri importanţi ai comunităţii de afaceri, specialişti cu experienţă, etc.) În plus, unii factori de decizie au o experienţă mai vastă în domeniul vizat decât analiştii de informaţii sau personalul din subordine.

Pe de altă parte, factorii de decizie sunt prea ocupaţi pentru a se ocupa de culegerea şi analizarea informaţiilor, dincolo de faptul că citesc ziarele, telegramele cu caracter secret (care nu pot fi lăsate în seama subordonaţilor) şi materialele selectate de personalul lor. În mod inevitabil, cele mai multe informaţii le vor fi transmise sub formă de extrase sau evaluări deja întocmite, prezentate oral sau în scris.

Spre deosebire de şefii lor, subordonaţii pot avea timpul necesar pentru a culege şi analiza multe dintre informaţiile necesare. Având în vedere că aceştia sunt implicaţi şi în procesul decizional, ei trebuie să ştie ce aspecte sunt relevante, care sunt obiectivele urmărite şi aşa mai departe. Cu excepţia chestiunilor secrete, ei au cunoştinţă de interacţiunile cu alte guverne sau alţi membri ai propriului guvern. În general, ei se bucură de încrederea şefilor lor; totuşi, pot exista cazuri în care superiorii doresc să analizeze anumite aspecte fără ca subordonaţii lor să aibă cunoştinţă de acest lucru.

Cu toate acestea, este posibil ca membrii personalului să se concentreze mai mult asupra elaborării strategiilor decât asupra culegerii şi analizării informaţiilor. În consecinţă, ei ar putea să nu acumuleze experienţa necesară în domeniul informaţiilor. În orice caz, aceste responsabilităţi pe linie de informaţii vor avea o pondere mai redusă decât cele referitoare la elaborarea strategiilor; angajaţii nu au în general timpul necesar pentru a-şi dezvolta nivelul de cunoştinţe dincolo de "capitalul intelectual" pe care îl deţineau deja la numirea în funcţie. De asemenea, ei nu au acces şi nici experienţa necesară în ceea ce priveşte sursele şi metodele specifice activităţii de informaţii; astfel, este posibil ca ei să nu poată corobora informaţiile obţinute de la serviciile secrete cu alte categorii de informaţii. Totodată, ei pot fi supuşi unor presiuni din partea superiorilor, care doresc să se asigure că analizele realizate corespund opţiunilor lor strategice sau deciziilor deja adoptate.

Pe de altă parte, analiştii de informaţii se concentrează exclusiv asupra sarcinilor ce le revin pe linie de informaţii şi nu sunt direct responsabili pentru alegerea anumitor strategii. Cariera lor profesională se desfăşoară numai în sfera informaţiilor, deşi adesea analiştii trebuie să îşi asume atribuţii manageriale pentru a putea evolua în plan profesional. Aceştia nefiind implicaţi în procesul decizional, factorilor de decizie le-ar putea fi mai uşor să le pună întrebări legate de opţiunile strategice, care sunt prea controversate pentru a fi dezbătute într-un cadru politic mai larg. Analiştii au acces şi sunt familiarizaţi cu sursele şi metodele specifice activităţii de informaţii şi sunt astfel în măsură să coroboreze informaţiile primite pe aceste canale cu alte informaţii. În cele din urmă, ei sunt (sau cel puţin ar trebui să fie) pregătiţi să evalueze dacă anumite informaţii aparent veridice sunt, de fapt, rezultatul eforturilor de dezinformare ale adversarilor.

Totuşi, analiştii de informaţii se confruntă şi cu anumite dezavantaje. Necunoaşterea opţiunilor strategice ale propriului guvern poate face ca rezultatul activităţii lor să fie mai puţin util decât ar fi în alte condiţii, deoarece îi reduce relevanţa şi oportunitatea şi, totodată, poate conduce la o subestimare a măsurii în care acţiunile altora anticipează sau sunt o reacţie la propriile acţiuni. În special, "tabuul" legat de analiza propriilor capacităţi sau strategii poate face dificilă conturarea unei imagini clare şi utile a "echilibrului de forţe" existent în raport cu partea adversă. În plus, analiştii de informaţii pot avea tendinţa de a ignora sursele de informaţii din afara canalelor secrete obişnuite, deoarece credibilitatea unor asemenea surse ar putea fi mai greu de stabilit, iar furnizorii de informaţii din afara aparatului guvernamental (cum ar fi oamenii de ştiinţă sau oamenii de afaceri) ar putea fi mai puţin dispuşi să coopereze cu un serviciu de informaţii decât cu o agenţie guvernamentală.

Probabil că nu va exista o soluţie unică aplicabilă în toate cazurile. Totuşi, ar putea fi util ca factorii de decizie să ia în considerare procedurile aplicate în acest domeniu de aparatul militar. De regulă, un comandant are în subordinea sa un ofiţer de informaţii ("G-2" în limbajul armatei SUA). Acest ofiţer este specializat în probleme de informaţii, dar el lucrează pentru comandantul său, şi nu pentru un serviciu de informaţii. El are sarcina de a obţine, analiza şi interpreta *toate* informaţiile relevante, indiferent dacă provin din surse secrete, din alte surse guvernamentale sau din surse deschise. În plus, datorită pregătirii sale şi relaţiilor pe care le are cu serviciile secrete, el poate fi mai mult decât un destinatar pasiv al informaţiilor; el poate căuta la nivelul serviciilor secrete informaţiile necesare comandantului său şi poate susţine priorităţile acestuia cu privire la culegerea şi diseminarea informaţiilor.

ACTIVITATEA DE INFORMAŢII ŞI DEMOCRAŢIA

Democraţia şi confidenţialitatea informaţiilor

Confidenţialitatea, aşa cum am remarcat deja, ridică o potenţială problemă în ceea ce priveşte exercitarea controlului asupra serviciilor de informaţii de către organismele de supraveghere din afara comunităţii de informaţii. Nevoia legitimă de a limita cunoaşterea unor detalii ale operaţiunilor desfăşurate la un cerc cât mai restrâns poate să ducă la camuflarea unor acţiuni neautorizate, împiedicând astfel autorităţile din afara comunităţii de informaţii să ia cunoştinţă de respectivele operaţiuni.

Într-o societate democratică, confidenţialitatea ridică însă şi o altă problemă: posibilitatea de a pune sub semnul întrebării legitimitatea politică a unui serviciu de informaţii, spre deosebire de controlul propriu-zis. Dacă democraţia reprezintă nu numai conducerea în interesul poporului, ci şi exercitarea ei de către popor, nu este de mirare că instituţiile pentru care confidenţialitatea este un aspect extrem de important pot deveni foarte uşor

ţinte ale neîncrederii populaţiei. Această suspiciune nu se limitează doar la serviciile secrete. Promisiunea făcută de Preşedintele Woodrow Wilson că problemele internaţionale ale perioadei de după primul război mondial aveau să fie soluţionate "prin înţelegeri publice, adoptate în urma unei dezbateri publice" reflecta suspiciunea oamenilor de rând faţă de diplomaţia antebelică şi faţă de confidenţialitate în general.

Controlul legislativ şi al societăţii civile

Scepticismul privind confidenţialitatea existentă la nivel guvernamental este probabil un fenomen endemic în societăţile democratice şi a condus în Statele Unite şi, într-o măsură mai mică, în alte ţări democratice, la necesitatea exercitării controlului asupra serviciilor de informaţii de către anumite organisme guvernamentale care se bucură de independenţă în raport cu şeful statului. În Statele Unite, s-a stabilit la mijlocul anilor '70 un sistem de control exercitat de către Congres prin intermediul a două comisii create în acest scop (Comisia Specială Permanentă a Camerei Reprezentanţilor pentru activitatea serviciilor de informaţii şi Comisia Specială a Senatului pentru activitatea serviciilor de informaţii).

Piatra de temelie a acestui sistem de control o constituie obligaţia legală a preşedintelui de a "informa permanent şi complet aceste comisii cu privire la activităţile de informaţii" desfăşurate de diverse structuri guvernamentale.[25] Dreptul celor două comisii de a fi informate este deosebit de important, ţinând cont şi de prerogativele Congresului cu privire la alocarea de fonduri. Potrivit lui Robert Gates, rezultatul este acela că, în anumite situaţii,

> procesul de control a conferit Congresului - în special celor două comisii pentru controlul activităţii serviciilor de informaţii – o cunoaştere mult mai amplă şi o influenţă mult mai mare decât a oricărei structuri din cadrul executivului asupra modului în care CIA şi alte servicii de informaţii îşi cheltuiesc banii, de la cheltuieli de ordinul miliardelor de dolari la achiziţii de ordinul miilor... În prezent, Congresul poate avea mai multă influenţă asupra priorităţilor CIA şi asupra modului de alocare a resurselor decât executivul.[26]

Sistemul de control exercitat de Congres poate fi privit ca un compromis între necesitatea păstrării confidenţialităţii şi de a spori influenţa opiniei publice asupra serviciilor de informaţii, astfel încât să se asigure că serviciile secrete nu utilizează mijloace şi nu urmăresc obiective pe care opinia publică le-ar dezaproba. Controlul exercitat de Congres permite comisiilor pe probleme de informaţii să fie un substitut al dezbaterii mai ample (în cadrul executivului, al Congresului şi în rândul populaţiei) care ar însoţi adoptarea altor strategii sau iniţiative guvernamentale.

Ambiguitatea creată prin utilizarea comisiilor ca substitut al opiniei publice este sesizată mai ales atunci când este vorba de acțiunile secrete, problemă care a condus de fapt la instituirea actualului sistem de control exercitat de către Congres. Baza legală pentru rolul comisiilor este cerința ca ele să fie notificate de fiecare dată când preşedintele ordonă o acțiune secretă. Deşi cerința notificării nu implică, în principiu, prerogative de veto, obiecțiile puternice ale membrilor comisiilor pot duce la revizuirea sau chiar la anularea unei propuneri de acțiune secretă atunci când consecințele politice ale unei astfel de acțiuni par să fie mai mari decât rezultatele estimate.[27] Astfel, unul dintre scopurile notificării prealabile poate fi descris ca fiind o testare a propunerii în fața unui segment (relativ restrâns) al opiniei politice, reprezentat de persoane independente de preşedinte, pentru a stabili dacă propunerea corespunde sau nu principiilor şi valorilor fundamentale.

Lăsând la o parte această funcție de substitut al dezbaterilor publice, transmiterea informațiilor referitoare la acțiuni secrete către membrii Congresului dă posibilitatea punerii în practică a prerogativelor Congresului în materie de alocare a fondurilor. Aceste prerogative pot fi exercitate de către comisiile pe probleme de informații sau pot implica o dezbatere la nivelul Senatului şi al Camerei Reprezentanților; aşa s-a întâmplat în cazul "amendamentelor Boland" prin care se limita sau se interzicea sprijinirea mişcării de rezistență din Nicaragua în anii '80.[28]

Principalul argument în favoarea exercitării controlului de către Congres asupra acțiunilor secrete este acela că întruneşte avantajele controlului democratic, pe de o parte, cu cele ale păstrării confidențialității, pe de altă parte. Analiza în cadrul comisiilor reprezintă un substitut al unei dezbateri publice efective şi al procesului democratic uzual de luare a deciziilor - acestea fiind, bineînțeles, incompatibile cu păstrarea confidențialității.

Valabilitatea acestui argument a fost însă contestată atât din perspectivă practică, cât şi teoretică. Practic, problema este dacă nu cumva controlul exercitat de către Congres nu conduce inevitabil la divulgarea informațiilor, indiferent de prevederile regulamentelor. De fapt, există puține date certe privind sursa numeroaselor scurgeri de informații legate de acțiunile secrete, iar investigarea anumitor cazuri de scurgeri de informații nu dă aproape niciodată rezultate. Având în vedere importanța pe care o acordă jurnaliştii păstrării confidențialității surselor, acest lucru nu este surprinzător.[29]

În orice caz, nu există nici o îndoială că sistemul de control al Congresului conduce la creşterea numărului persoanelor care au acces la informațiile privind acțiunile secrete. În general, riscul unei scurgeri de informații depinde de numărul de persoane care au acces la informații. De asemenea, congresmenii şi personalul din subordinea lor sunt, de regulă, mai puțin obişnuiți să lucreze cu informații clasificate şi îşi desfăşoară activitatea într-un mediu cu un caracter politic mai pronunțat decât cel specific unui ofițer de informații. Cerința de a informa Congresul presupune probabil

implicarea unor persoane din cadrul executivului, având în vedere că trebuie să fie puse în temă şi o serie de persoane care se ocupă de relaţiile administraţiei cu Congresul. În majoritatea cazurilor, un număr destul de mare de angajaţi din cadrul executivului au acces la informaţii, astfel încât, după toate probabilităţile, creşterea numărului celor care intră în posesia informaţiilor ca urmare a controlului exercitat de Congres nu măreşte semnificativ riscul unor scurgeri de informaţii; în cazuri speciale, când accesul este limitat la un număr restrâns de persoane din cadrul executivului, odată cu creşterea numărului celor care iau cunoştinţă de informaţiile respective, creşte şi riscul producerii unor scurgeri de informaţii.

Deşi, în mare parte, dezbaterea publică declanşată pe marginea controlului exercitat de Congres odată cu instituirea acestui sistem privea scurgerile de informaţii, problema de natură teoretică legată de acest sistem de control asupra acţiunilor secrete priveşte necesitatea şi eficienţa adoptării de către Congres a unor proceduri secrete ca activitate de rutină.

Astfel, un fost oficial al Uniunii pentru Libertăţile Civile din America, Morton Halperin, a depus mărturie în faţa Comisiei Church, aducând argumente împotriva conceptului:

> [Aplicarea unor forme mai bune de control] nu reuşeşte să elimine dezavantajele inerente deţinerii unor atribuţii în ceea ce priveşte derularea acţiunilor secrete. Singura armă pe care o au la dispoziţie opozanţii unei politici prezidenţiale, din interiorul sau din afara executivului, este dezbaterea publică. Dacă o strategie poate fi dezbătută public, atunci Congresul poate fi convins să exercite presiuni asupra preşedintelui, iar presiunile din partea opiniei publice pot determina o schimbare de strategie. Dar, dacă se acceptă legitimitatea ideii de confidenţialitate, atunci măsurile de control asupra operaţiunilor secrete pot fi ignorate cu uşurinţă.[30]

Deşi această apreciere s-a dovedit a nu lua în considerare rezultatele pe care le pot obţine comisiile Congresului prin negocieri fără caracter public cu executivul (existând permanent ameninţarea dezvăluirii informaţiilor), ea conţine un sâmbure de adevăr: în cazul unor divergenţe majore de opinii, cum ar fi sprijinul "secret" acordat mişcării de rezistenţă din Nicaragua în anii '80, s-a renunţat la păstrarea confidenţialităţii şi problemele au fost dezbătute de Congres în mod public.

Astfel, ideea controlului exercitat de Congres în condiţiile păstrării confidenţialităţii include o contradicţie în termeni: se urmăreşte obţinerea beneficiilor aferente deliberării problemelor de informaţii în cadrul legislativului, dar se exclude de la bun început principala metodă utilizată într-o astfel de deliberare – dezbaterea amplă, cu caracter public.

Aceste aspecte privind păstrarea confidenţialităţii şi controlul activităţii de informaţii se confundă adesea cu o altă chestiune, total diferită: în ce măsură faptul că un stat este democratic influenţează politica externă

pe care ar trebui să o adopte? Acest lucru este valabil, în special, cu privire la acțiunile secrete, aspect al activității de informații care, în Statele Unite, a atras cele mai multe critici pe motiv că ar fi antidemocratice. Totuşi, majoritatea criticilor la adresa CIA privind acțiunile secrete desfăşurate ar fi trebuit să fie îndreptate mai degrabă împotriva strategiilor de politică externă care prevedeau astfel de acțiuni.

În Statele Unite, principala nemulțumire legată de acțiunile secrete din anii '70 şi '80 viza faptul că reprezentau un amestec în treburile interne ale altor țări. Caracterul secret sau public al intervenției respective era, se pare, un aspect secundar. S-a argumentat uneori că o asemenea acțiune este nedemocratică, în sensul că se realizează în secret tocmai pentru că ar fi întâmpinat o opoziție puternică din partea opiniei publice dacă ar fi fost cunoscută. Situația nu este însă atât de clară precum pretind cei care invocă aceste argumente. De exemplu, diferitele acțiuni secrete îndreptate împotriva lui Fidel Castro, inclusiv tentativele de asasinat, s-ar fi putut bucura de sprijin popular la momentul la care au avut loc. Atunci când Comisia Church a obiectat că aceste acțiuni nu beneficiau de susținerea opiniei publice americane, aceasta a analizat acțiunile secrete întreprinse în trecut de CIA nu prin raportare la opinia publică de la sfârşitul anilor '50 şi începutul anilor '60 (atunci când au avut loc tentativele), ci la opinia publică de după războiul din Vietnam, de la mijlocul anilor '70.[31] În jurul anilor '90, opinia publică a înregistrat o nouă schimbare, acceptând cu uşurință intervenția SUA în treburile interne ale statelor Haiti şi Iugoslavia (cu privire la Kosovo).

De la mijlocul anilor '70, când au fost înființate comisiile de control pe probleme de informații din cadrul Congresului SUA, şi alte țări democratice au avut în vedere constituirea unor organisme independente de control asupra activității de informații. De exemplu, în 1984, Parlamentul canadian a înființat Comisia de analiză a activităților de informații privind securitatea (SIRC), pentru exercitarea controlului asupra aparatului intern de informații, care a fost separat de Serviciul Regal Canadian al Poliției Călare şi a fost transformat într-o agenție civilă, Serviciul Canadian de Informații privind Securitatea.

Spre deosebire de comisiile de control din SUA, SIRC nu este o comisie a parlamentului, ci este alcătuită din consilieri numiți de primul ministru în urma unor consultări cu liderii partidelor de opoziție. (Consiliul privat este un grup ai cărui membri, de obicei foşti membri ai cabinetului, au fost recunoscuți oficial de către guvernul canadian în calitate de consilieri). SIRC prezintă un raport anual în fața Parlamentului, dar nu are prerogative legislative sau în materie de buget. Diferența dintre mecanismele de control din Canada şi SUA reflectă diferențele dintre cele două sisteme politice; în sistemul american, principalele divergențe apar între executiv şi legislativ, ceea ce nu se întâmplă în sistemul parlamentar canadian, care se caracterizează printr-o puternică disciplină de partid. (În astfel de sisteme, primul ministru este liderul partidului sau al coaliției de partide ce deține majoritatea locurilor în Parlament şi este el însuşi membru al Parlamentului).

În Canada, independența necesară față de puterea executivă se obține cu sprijinul unor eminenți oameni de stat.[32]

Alte țări, printre care Marea Britanie, Australia,[33] Noua Zeelandă şi Germania au creat comisii parlamentare cu atribuții de control, deşi aceste comisii se deosebesc în mai multe privințe de modelul SUA.[34] Principala diferență, aşa cum am arătat mai sus, este aceea că respectivele sisteme parlamentare nu permit o independența legislativă inerentă sistemului prezidențial al Statelor Unite, caracterizat prin separarea dintre puterea executivă şi cea legislativă. Astfel, în Marea Britanie, membrii Comisiei pentru Informații şi Securitate sunt "numiți de către primul ministru, în urma consultărilor cu liderul opoziției" ("opoziția" fiind partidul sau coaliția minoritară din Parlament).[35] De asemenea, comisia îl informează pe primul ministru, care, înainte de a prezenta informarea Parlamentului, "poate să excludă materialele care consideră că ar aduce atingere îndeplinirii atribuțiilor agenților, după ce se consultă cu membrii Comisiei".[36]

În plus, sfera de responsabilitate a acestor comisii este diferită. Astfel, conform legii sale de înființare, competențele de investigații ale Comisiei Parlamentare Comune pentru Controlul Agenției Australiene de Informații şi Securitate (ASIO) nu cuprind şi "aspecte ce țin de obținerea sau comunicarea de către ASIO a informațiilor externe" sau "aspectele activității ASIO care nu afectează cetățenii australieni sau persoanele cu rezidență permanentă".[37]

Democrația, activitatea de contrainformații şi informații interne

De fapt, contrainformațiile, nu acțiunile secrete, este elementul activității de informații care este cel mai puternic afectat de natura democratică a regimului pe care îl deserveşte. Cele mai multe dintre dificultățile care apar în relația dintre democrație şi activitatea de informații privesc contrainformațiile. Aceste dificultăți privesc, în special, stabilirea situațiilor în care o agenție guvernamentală poate realiza în mod legitim supravegherea cetățenilor statului respectiv şi a eventualelor limite ale unei astfel de supravegheri.

În Statele Unite această discuție tinde să fie purtată în termeni de drept constituțional. De exemplu, se ridică problema modului în care ar trebui interpretată, în cazuri ce privesc siguranța națională, interdicția conținută în cel de-al patrulea Amendament la Constituția Americană[38] referitoare la percheziții şi confiscări nejustificate. Se punea şi problema legitimității interceptării comunicațiilor telefonice (care sunt considerate o formă de percheziție) în cazuri ce țin de siguranța națională: în cazul acestor interceptări realizate din rațiuni de siguranță națională, trebuie aplicată cerința obținerii în prealabil a unui mandat judecătoresc? Această întrebare şi-a găsit răspunsul în Legea din 1978 privind informațiile externe (FISA). În această lege era prevăzută condiția obținerii în prealabil a unui mandat judecătoresc pentru interceptări în cazurile de siguranță națională, dar se înființa o instanță specială care emitea astfel de mandate şi care funcționa

conform unor proceduri menite să protejeze confidențialitatea întregului proces.[39] În 1994 s-a introdus o procedură similară pentru percheziţiile corporale în cazuri de siguranţă naţională.[40]

Deşi s-a acordat o atenție deosebită acceptării sau neacceptării diferitelor mijloace de derulare a activității de contrainformații (mijloace despre care nu vom discuta în detaliu aici), au fost neglijate o serie de probleme esențiale privind scopurile activității de contrainformații sau ale activității serviciilor de informații interne într-o societate democratică.[41] Cu alte cuvinte, ce fel de informații sunt necesare? Care este scopul pe care îl deservesc aceste informații? Ce tipuri de amenințări impun desfăşurarea acțiunilor de culegere de informații pe plan intern?

Este foarte dificil de găsit un răspuns la aceste întrebări atunci când este vorba de un stat democratic, spre deosebire de un stat cu regim totalitar. În acest din urmă caz, orice opoziție la adresa conducerii de stat constituie, în principiu, un element de interes pentru activitatea de informații. Monitorizând în mod constant opoziția, conducerea statului se asigură că poate lua toate măsurile necesare pentru a rămâne la putere, fie prin intermediul sistemului obişnuit de aplicare a legii, fie prin mijloace din afara acestui sistem.

Pe de altă parte, într-un stat democratic, simpla opoziție față de conducerea statului de la un anumit moment nu este şi nu trebuie considerată o amenințare la adresa țării sau a sistemului ei de guvernământ. Interesele de securitate națională ale unei țări (spre deosebire de interesele de ordin politic ale conducerii statului) nu sunt amenințate de simpla existență a opoziției şi nu se impune desfăşurarea unei activități de culegere de informații pe plan intern cu privire la aceste aspecte. Se pune atunci întrebarea care sunt acțiunile care constituie potențiale amenințări la adresa siguranței naționale şi impun culegerea de informații în această privință?

În special, unde trebuie trasă linia de demarcare între acțiunile care fac obiectul legitim al activității de culegere de informații şi cele lipsite de legitimitate? Activitatea de informații trebuie să aibă în vedere opiniile propriu-zise ale unei persoane sau doar situațiile în care aceste opinii sunt însoțite de acțiuni? Criteriul ar trebui să fie acela al legalității sau ilegalității acțiunii? Există acțiuni care, deşi sunt legale, trebuie să fie cunoscute de către conducerea statului şi, în consecință, pot fi supravegheate într-un fel sau altul?

Standardul în materie de infracționalitate. Datorită atenției prioritare acordate *mijloacelor* utilizate în culegerea de informații pe plan intern (mai ales în privința constituționalității sau neconstituționalității acestor mijloace), în detrimentul *scopurilor*, aceste probleme nu au fost abordate în mod explicit în dezbateri publice privind activitatea de informații. Totuşi, s-a dat oarecum un răspuns la mijlocul anilor '70, în Statele Unite (în perioada de desfăşurare a investigațiilor privind activitatea de informații la nivelul Congresului); s-a încercat atunci aplicarea a ceea ce s-a numit "standardul în materie de infracționalitate" în activitatea serviciilor

de informații interne. Cu alte cuvinte, investigațiile specifice serviciilor de informații interne se declanşau doar atunci când avusese sau urma să aibă loc o încălcare a legii. Consecința a fost că obiectul de activitate al serviciilor de informații interne urma să fie delimitat de lege; o acțiune ilegală poate constitui obiectul activității de culegere de informații, dar o acțiune legală nu poate face obiectul unor astfel de cercetări.[42] Deşi acest principiu nu a fost niciodată promovat într-o manieră foarte explicită, el a deschis calea recomandărilor date de către ministrul de justiție în 1976. Impactul acestui principiu poate fi observat şi în textul Legii din 1978 privind informațiile externe, singurul act legislativ adoptat de Congres în acest domeniu în perioada respectivă.[43]

Aceste recomandări au fost date de Edward Levi, ministrul de justiție din perioada respectivă, precizându-se situațiile în care FBI putea utiliza diferite tehnici de supraveghere şi investigare. În scopul elaborării acestor recomandări, domeniul informațiilor interne a fost împărțit în două zone: securitatea internă, pe de o parte, şi informațiile externe şi contrainformațiile, pe de altă parte; au fost emise recomandări diferite pentru investigațiile aferente fiecăruia dintre aceste domenii.

Recomandările pentru investigațiile din domeniul informațiilor externe şi contrainformațiilor sunt clasificate şi nu au fost niciodată făcute publice în totalitate.[44] De aceea, este dificil de stabilit în ce măsură aceste recomandări aplică standardul în materie de infracționalitate în cadrul investigațiilor în care sunt aplicabile. Marea majoritate a investigațiilor realizate în baza acestor recomandări privesc identificarea şi prevenirea acțiunilor de spionaj. Astfel, investigațiile se concentrează asupra activităților cu potențial de infracționalitate. Acelaşi lucru este valabil pentru depistarea şi prevenirea acțiunilor teroriste desfăşurate sub comandă externă, aceasta constituind probabil cealaltă misiune prioritară a FBI, care trebuie îndeplinită conform acestor recomandări.

Nu este clar în ce măsură recomandările au în vedere investigarea acțiunilor politice legale desfăşurate în numele unui guvern străin, şi anume desfăşurarea de acțiuni secrete sau măsuri active luate de un guvern străin şi îndreptate împotriva Statelor Unite. Este adevărat că, în conformitate cu recomandările,

> *cu respectarea standardelor şi procedurilor aprobate prin aceste recomandări*, FBI este autorizat să depisteze şi să prevină acțiunile de spionaj, sabotaj şi *alte acțiuni clandestine de informații* derulate de puteri străine sau sub îndrumarea acestora, prin operațiuni legale de contrainformații desfăşurate pe teritoriul Statelor Unite, inclusiv prin supraveghere electronică, operațiuni care sunt necesare sau utile în vederea atingerii obiectivelor.[45]

Aceasta înseamnă că activități în general legale, cum ar fi propaganda politică, activitățile desfăşurate de diverse organizații şi colectarea de

fonduri, fac obiectul supravegherii atunci când sunt realizate de o putere străină sau sub îndrumarea acesteia. De asemenea, cel puțin teoretic, oricine desfăşoară o astfel de activitate în numele unui guvern străin este obligat să se înregistreze ca agent străin, în conformitate cu Legea de înregistrare a agenților străini (FARA), neînregistrarea fiind o infracțiune.[46]

Pe de altă parte, neînregistrarea nu constituie decât rareori singurul motiv pentru care se declanşează o investigație a serviciilor de contrainformații sau se începe urmărirea penală.[47] Probabil că singura investigație de acest gen a privit Comisia pentru solidaritate cu poporul din El Salvador (CISPES), care a făcut obiectul unei verificări derulate de FBI timp de trei luni în 1981. Investigația a avut loc la cererea Direcției penale a Departamentului de Justiție "pentru a stabili dacă CISPES trebuie să se înregistreze conform" legii FARA ca agent al Frente Democratio Revolucionario din Salvador, aripa politică a mişcării de gherilă din El Salvador.[48] Având în vedere însă că acesta a fost un caz excepțional, este neclar (cel puțin prin prisma informațiilor publice disponibile) în ce măsură standardele şi procedurile aprobate prin aceste recomandări permit o investigare eficientă a activităților clandestine de informații care nu implică acțiuni de violență sau încălcarea vreunei legi (alta decât FARA).

Spre deosebire de recomandările privind activitatea de contrainformații, cele privind securitatea internă (denumite "recomandările Levi") au fost făcute publice.[49] Acestea privesc, în primul rând, investigarea grupărilor care au fost denumite la un moment dat "subversive" sau "anti-americane". Deşi aceşti termeni sunt imprecişi, se includ aici grupări: (1) ostile nu doar guvernului aflat la putere şi politicilor acestuia, ci şi structurii constituționale şi principiilor sale fundamentale, (2) grupări care urmăresc încălcarea drepturilor civile ale anumitor categorii de persoane (cum ar fi grupurile rasiale, etnice sau religioase) sau (3) grupări care urmăresc înlăturarea conducerii politice prin mijloace violente.

Elementul-cheie al recomandărilor lui Levi este acela că investigarea activității acestor grupări este permisă doar atunci când o grupare (sau un individ) este implicată sau se poate implica în activități "care presupun sau vor presupune utilizarea forței sau a violenței şi care presupun sau vor presupune încălcarea legislației federale"[50] Acesta este, în esență, standardul în materie de infracționalitate, care stabileşte cu claritate sfera de interes a guvernului în domeniul securității interne.

Cel mai important motiv pentru adoptarea acestui standard a fost acela de a garanta că nu se întreprinde nici o acțiune de supraveghere doar pentru că o persoană sau un grup îşi exercită dreptul de liberă exprimare, dreptul la libertatea presei sau dreptul de liberă asociere, prevăzute în Primul Amendament la Constituția SUA.[51] Există două argumente care justifică acest obiectiv. În primul rând, există opinia potrivit căreia o investigație guvernamentală întreprinsă asupra unei persoane sau a unui grup constituie în sine o sancțiune care nu ar trebui să se aplice celor care nu au comis nici o ilegalitate. Cel de-al doilea argument evidențiază faptul că acest tip de investigație, fie din cauza caracterului său neplăcut pentru cel vizat, fie din

cauză că pare să anunțe o pedeapsă ulterioară, "îngheață" în mod inevitabil activitatea (exercitarea dreptului) care face obiectul supravegherii. Aceste motive sunt plauzibile într-o anumită măsură, dar nu sunt întotdeauna foarte convingătoare. În termeni constituționali, se pune întrebarea dacă supravegherea realizată în asemenea condiții reprezintă o restrângere a libertăților garantate de Primul Amendament.

Această problemă nu poate fi tratată aici pe larg. Câteva elemente ilustrează însă argumentele pro şi contra adoptării standardului în materie de infracționalitate. Pe de o parte, încălcarea dreptului la viață privată, pe care o presupune urmărirea unei persoane de către agențiile guvernamentale, este într-adevăr dezagreabilă. Totuşi, acelaşi lucru este valabil pentru toate investigațiile întreprinse de agențiile de aplicare a legii care vizează persoane ce nu sunt suspectate de a fi comis o anumită infracțiune: verificările privind impozitul pe venit, inspecțiile vamale şi multe alte acțiuni ale organelor de aplicare a legii constituie un amestec în viața privată, dar guvernul este autorizat şi chiar întreprinde astfel de măsuri, fără a avea motive să suspecteze că persoana vizată a comis vreo infracțiune.

De asemenea, posibilitatea unei supravegheri întreprinse de către agențiile guvernamentale ar putea să descurajeze activitățile politice controversate, deoarece ar exista temerea că includerea numelor persoanelor implicate într-un dosar ar putea da naştere unor probleme în viitor. Totuşi, efectul restrictiv al unei investigații secrete care nu se finalizează prin întreprinderea unei acțiuni nu poate fi decât unul minim. Efectul pare să fie mai degrabă echivalent oprobriului public pe care o persoană şi l-ar atrage dacă ar îmbrățişa idei lipsite de popularitate, decât cel de limitare a libertăților prevăzute în primul Amendament. Potrivit dreptului constituțional, Curtea Supremă a respins opinia conform căreia o persoană are de suferit ca urmare a "simplei existențe a unei acțiuni guvernamentale de investigații şi de culegere de informații." Curtea a hotărât că, în ceea ce priveşte îndeplinirea condițiilor legale pentru a contesta o investigație guvernamentală în fața instanței, "afirmațiile privind efectul restrictiv subiectiv [ca urmare a desfăşurării unei investigații guvernamentale secrete] nu pot substitui în mod adecvat existența unei vătămări concrete, obiective, sau riscul produceri unei astfel de vătămări în viitor."[52]

Aşa cum remarca Kenneth Robertson, această problemă este dezbătută, în general, din punct de vedere al interdicțiilor prevăzute de dreptul constituțional cu privire la anumite tipuri de acțiuni guvernamentale. De asemenea, trebuie să se analizeze dacă aceste standarde permit guvernului să îşi satisfacă nevoile legitime de informații cu privire la evenimentele ce au loc în societate.[53] În cel puțin două domenii de interes, se poate argumenta că, cel puțin teoretic, aceste standarde nu acordă guvernului suficientă libertate de acțiune.

Standardul în materie de infracționalitate şi securitatea personalului. Primul dintre aceste domenii priveşte programul guvernului de asigurare a securității personalului, program menit să verifice potențialii sau

actualii angajaţi guvernamentali înainte de a le acorda acces la informaţii clasificate. În acest scop, guvernul este îndreptăţit să ştie dacă respectivii candidaţi au afilieri sau legături care i-ar putea determina să divulge informaţii clasificate reprezentanţilor unor puteri străine sau să acţioneze în alt mod împotriva intereselor ţării. În general, aceste aspecte sunt dificil de stabilit în cadrul verificărilor, din motivele enumerate în capitolul 5. Singura posibilitate ca guvernul să poată afla cu o anumită certitudine dacă respectivul candidat are o astfel de afiliere este ca instituţiile guvernamentale să aibă şi alte surse de informaţii provenind din supravegherea organizaţiilor respective.

În această privinţă, este important să înţelegem în ce anume constă protecţia asigurată de Primul Amendament. Conform hotărârii Curţii Supreme în cazul *Brandenburg vs. Ohio*, este protejată "susţinerea la nivel teoretic" a ideii răsturnării guvernului SUA. Susţinerea unor astfel de idei poate fi interzisă doar atunci când "aceste idei sunt menite să incite sau să provoace acţiuni anarhiste *iminente* şi există probabilitatea incitării sau provocării unor astfel de acţiuni".[54] Conform unui standard strict în materie de infracţionalitate, o organizaţie care încurajează răsturnarea prin violenţă a guvernului SUA nu poate face obiectul supravegherii decât atunci când acţiunile sale trec de la nivelul abstract la cel concret, aşa cum am explicat mai sus.

În plus, apartenenţa la o organizaţie care desfăşoară acţiuni concrete de promovare poate avea caracter de infracţionalitate doar dacă persoana respectivă este membru activ şi dacă are "cunoştinţă despre activitatea ilegală de promovare desfăşurată de organizaţie şi dacă are intenţia clară de a provoca răsturnarea prin violenţă a guvernului SUA 'cât de rapid posibil în circumstanţele date.'"[55] Acest lucru înseamnă că, dacă s-ar respecta un anumit standard în materie de infracţionalitate, ar fi imposibilă supravegherea unei asemenea organizaţii în vederea elaborării unei liste complete a membrilor acesteia, din moment ce nu ar exista probe care să demonstreze că fiecare dintre membrii organizaţiei se încadrează în standardul de infracţionalitate, chiar dacă organizaţia, în ansamblu, corespunde criteriului *Brandenburg*.

Într-o oarecare măsură, imposibilitatea realizării unor liste cu numele membrilor organizaţiilor "subversive" (acele organizaţii care, date fiind obiectivele lor, pun sub semnul întrebării capacitatea membrilor de a obţine acces la informaţii clasificate) a fost rezultatul urmărit prin adoptarea standardului în materie de infracţionalitate. Aşa cum remarca John Elliff, prezentând deciziile iniţiale ale ministrului de justiţie Edward Levi:

> Levi a respins ideea că programul de securitate pentru angajaţii din structurile federale poate constitui baza investigaţiilor informative realizate de FBI. După părerea lui Levi, Ordinul Executivului (privind programul de securitate a personalului) autoriza Biroul doar să investigheze angajaţii şi candidaţii pentru executiv. Ordinul nu constituia temeiul în baza căruia FBI să poată desfăşura investigaţii informative pe plan intern.[56]

Cu alte cuvinte, investigaţiile nu pot porni de la acţiunile sau declaraţiile publice ale unui grup. Ele trebuie să înceapă doar dacă există o solicitare de ocupare a unui post în structurile administrative din partea unei persoane a cărei afiliere la o grupare poate fi camuflată.

Fără a supraveghea astfel de grupări în scopul întocmirii unei liste a membrilor lor, guvernul federal nu poate, în general, să ia măsurile necesare pentru a avea certitudinea că nu acordă acces la informaţii confidenţiale sau nu numeşte în posturi importante persoane care sunt membre ale unor partide politice loiale unei puteri străine ostile, membre ale unor grupări religioase ce dau dovadă de un devotament fanatic pentru liderii lor, ale căror scopuri reale ar putea să nu fie compatibile cu ideea de guvernare constituţională sau membre ale unor grupări ostile care vor să excludă anumite categorii de cetăţeni americani din rândul clasei politice. Acest lucru poate sau nu să reprezinte o problemă la un moment dat, în funcţie de existenţa unor astfel de grupări şi de măsura în care acestea sunt capabile să elaboreze o strategie menită să ascundă legătura membrilor lor cu gruparea şi să îi plaseze în funcţii guvernamentale importante ("infiltrându-se" în guvern).[57]

Standardul de infracţionalitate şi antiterorismul. Situaţia este întrucâtva diferită în cazul grupărilor teroriste. Deşi o grupare teroristă activă poate face obiectul supravegherii indiferent de standardul de infracţionalitate aplicat, poate fi extrem de dificilă instituirea unei astfel de supravegheri în cazul unor grupări sofisticate, aşa cum sunt majoritatea grupărilor teroriste existente în ultimele decenii în Orientul Mijlociu şi Europa Occidentală. Având în vedere cât de puţine informaţii pot fi obţinute prin mijloace tehnice cu privire la locaţiile stabile şi mijloacele de comunicaţie ale acestor grupări, cea mai utilă tehnică de culegere de informaţii este infiltrarea de agenţi într-o grupare. O grupare sofisticată va fi însă precaută cu privire la persoanele din afară şi va avea încredere doar în acele persoane cu care membrii actuali au avut relaţii personale îndelungate sau care şi-au dovedit devotamentul faţă de grupare prin comiterea unor infracţiuni grave. Doar şansa poate ajuta un serviciu de informaţii ca, pornind de la zero, să îşi infiltreze agenţii într-o grupare teroristă deja organizată şi operaţională.

Serviciile de informaţii trebuie să recurgă la alte strategii pentru a rezolva această problemă. În primul rând, serviciile trebuie să poată culege informaţii despre grupurile de sprijin - simpatizanţi care asigură susţinere financiară, logistică, politică şi juridică, dar nu iau parte la activităţile teroriste propriu-zise.

Infiltrarea într-un grup de sprijin, deşi mai simplu de realizat, nu este la fel de avantajoasă ca infiltrarea în gruparea teroristă. Cu toate acestea, ea poate fi foarte utilă; în funcţie de tipul sprijinului acordat, se poate deduce momentul şi natura unor viitoare acte teroriste. În plus, un membru al unui grup de sprijin, prin legăturile sale personale sau prin recrutarea de către gruparea teroristă, poate să ajungă într-o poziţie din care să poată furniza informaţii de o mai mare precizie. Un agent infiltrat într-un grup de sprijin poate fi în măsură să împiedice comiterea uni act terorist, fie furnizând

poliției o informație-cheie (cum ar fi descrierea mașinii închiriate care urmează să fie utilizată în actul terorist), fie sabotând direct atentatul cu bombă (de exemplu, înlocuind praful de pușcă cu rumeguș) sau alte echipamente. Așa cum explica Shlomo Gazit, fost director al serviciului israelian de informații,

> Sunt foarte puține organizațiile [teroriste] care pot funcționa într-un sistem de compartimentare totală și care nu depind de rețele locale de sprijin. Aceste rețele sprijină organizația teroristă fie din rațiuni ideologice, fie ca urmare a unor acțiuni de intimidare și șantaj, fără a se implica direct în operațiunile teroriste. Importanța infiltrării în rețelele de simpatizanți și susținători rezidă în faptul că aceasta este mult mai simplu de realizat decât infiltrarea în organizațiile teroriste, care sunt mult mai greu accesibile. Infiltrarea în aceste rețele de sprijin poate face posibilă infiltrarea în organizația propriu-zisă sau obținerea de informații indirecte despre aceasta.[58]

Standardul în materie de infracționalitate împiedică infiltrarea în grupurile de sprijin deoarece acestea se prezintă în general sub forma unor grupări politice sau caritabile, ceea ce și sunt, parțial. Un grup de sprijin poate susține că este implicat în acțiuni de propagandă politică în favoarea unor cauze care sunt, întâmplător, și cauzele îmbrățișate de gruparea teroristă. În mod similar, un alt grup poate susține că activitatea sa are ca scop sprijinirea soțiilor și copiilor unor presupuși teroriști care au fost închiși sau uciși. Un alt grup poate susține că se limitează la asigurarea asistenței juridice și a fondurilor necesare pentru apărarea teroriștilor puși sub acuzare.

Fără infiltrarea unui informator în grupul de sprijin, ar putea fi imposibil să se stabilească natura exactă a activităților secundare (și deloc inocente) desfășurate de grupul de sprijin în numele organizației teroriste. Dar utilizarea unei asemenea metode intruzive sau a altei tehnici similare este permisă doar dacă există deja probe privind implicarea grupului în acțiuni violente, infracționale.[59] În această privință, standardul în materie de infracționalitate dă naștere unui cerc vicios: nu se pot cunoaște activitățile secundare desfășurate de un grup, pentru că nu pot fi investigate, și nu pot fi investigate deoarece nu există informații despre derularea unor astfel de activități.

O a doua modalitate de depășire a problemei legate de supravegherea grupărilor teroriste se bazează pe faptul că grupările teroriste sunt, în general, ramuri ale grupărilor extremiste, naționaliste sau separatiste; ele sunt alcătuite, de obicei, din membri ai unor astfel de grupări, care sunt nemulțumiți de faptul că nu reușesc să își atingă obiectivele prin mijloace mai puțin violente. Prin infiltrarea unor informatori în rândul organizațiilor din care se pot desprinde grupări teroriste se poate cunoaște imediat existența unei noi grupări teroriste și se pot infiltra agenți în cadrul acestora încă de la

început. Pe de altă parte, un standard în materie de infracționalitate face imposibilă menținerea supravegherii inițiale, pe baza căreia pot fi obținute primele indicii referitoare la o nouă grupare teroristă.

O componentă aparte a activității de combatere a terorismului o reprezintă responsabilitatea Serviciului Secret american de a asigura protecția președintelui, a altor înalți demnitari, precum și a demnitarilor străini. Scopul acestei activități ca, de altfel, al întregii activități de combatere a terorismului, constă mai degrabă în a preveni un act criminal decât în a riposta la o astfel de acțiune prin pedepsirea făptuitorilor, astfel încât să se evite viitoare acțiuni de acest gen. Responsabilitatea Serviciului Secret presupune deținerea unor informații despre posibile tentative de asasinat care vizează persoanele aflate sub protecția sa. Standardul în materie de infracționalitate aplicabil în cazul investigării grupărilor care pot fi implicate în asasinate presupune că Serviciul Secret nu va primi avertizări cu privire la posibile tentative de asasinat decât după ce gruparea a inițiat deja o acțiune violentă, moment în care deținerea acestor informații ar putea fi tardivă. În 1982, un oficial din cadrul Departamentului Trezoreriei, responsabil de relația cu serviciul, a explicat problema astfel: "În ziua de azi, Serviciul Secret trebuie să manifeste preocupare față de intențiile şi activitățile grupărilor teroriste sau ale altor grupări extremiste. Trebuie să cunoaştem acest tip de amenințare înainte ca ea să se materializeze, şi nu după aceea."[60]

De asemenea, oficialul a remarcat faptul că, pentru o alocare adecvată a resurselor, serviciul trebuie să "ştie că, de exemplu, o organizație care are un discurs extremist fie nu disponibilitatea necesară transpunerii în practică a mesajului său, fie este incapabilă să declanşeze acțiuni periculoase". În opinia sa,

> problema actuală este că FBI nu este capabil să culeagă suficiente informații, lucru care se datorează, în parte, recomandărilor privind securitatea internă, promovate de ministrul de justiție, Levi. Anterior emiterii acestor recomandări, Serviciul Secret primea de la FBI numeroase informații secrete despre anumite persoane şi grupări care puteau recurge la acte de violență. Deşi s-a considerat că, în felul acesta, Serviciul Secret a beneficiat de prea multe informații - fiind nevoit să facă o selecție dintr-un volum mare de informații - situația era ideală din punctul de vedere al Serviciului Secret.
>
> Actuala problemă constă în faptul că nu se realizează o serie de investigații în anumite domenii importante. Rezultă de aici o lipsă de informații referitoare la locația, structura, planurile şi activitățile unor grupări care nu pot fi etichetate drept teroriste, dar care au o orientare radicală, sprijină cauzele organizațiilor teroriste şi pot recurge la acțiuni violente sau teroriste.

Desigur, această abordare generală este valabilă în cazul tuturor agenţiilor de aplicare a legii; în general, activitatea acestor agenţii vizează doar în mică măsură prevenirea infracţiunilor, concentrându-se cu precădere asupra depistării activităţilor infracţionale după comiterea acestora şi asupra pedepsirii autorilor. Este imposibil ca agenţiile obişnuite de aplicare a legii să îşi stabilească drept obiectiv prevenirea infracţiunilor, prin crearea unei reţele informative care să le avertizeze în legătură cu plănuirea unor acţiuni infracţionale. În ceea ce priveşte combaterea terorismului şi protecţia demnitarilor, din cauza gravităţii pe care o poate avea chiar şi un singur incident, există o disponibilitate sporită de a preveni infracţiunile şi nu doar de a le sancţiona, fapt ce implică necesitatea culegerii de informaţii despre persoane sau grupări care, deşi nu au comis acţiuni violente, se pot implica în astfel de activităţi sau pot menţine strânse legături cu cei care comit astfel de acţiuni.

În 1995, în urma atentatului cu bombă asupra sediului FBI din Oklahoma City, care s-a soldat cu un număr mare de victime, s-a pus din nou întrebarea dacă recomandările în materie de combatere a terorismului pe plan intern conferă FBI suficiente competenţe. Cu toate acestea, ministrul justiţiei, Janet Reno, şi Louis Freeh, directorul FBI, au considerat că revizuirea acestor norme nu este necesară, anunţând că prevederile în vigoare la momentul respectiv (recomandările lui Levy fuseseră revizuite de ministrul justiţiei, William French Smith, în 1983) urmau să beneficieze de o interpretare mai puţin restrictivă; prevederile respective stabileau posibilitatea declanşării unei investigaţii pe probleme de antiterorism atunci când "în baza faptelor şi împrejurărilor existente, se poate trage concluzia că două sau mai multe persoane sunt implicate într-o acţiune care vizează atingerea unor obiective politice sau sociale prin utilizarea forţei sau violenţei şi nerespectarea legislaţiei penale a SUA."[61] Potrivit lui Freeh, această reinterpretare avea să „permită FBI să demareze o investigaţie în cazul unei grupări care recurge la violenţă pentru a-şi atinge obiectivele politice sau sociale, fără a încălca însă legislaţia federală, dacă există indicii că respectiva grupare are capacitatea de a-şi atinge scopurile.”[62]

Deşi criteriul existenţei unor "indicii temeinice" este suficient de general pentru a include şi interpretarea lui Freeh (potrivit căreia nu trebuie să existe neapărat date privind o încălcare iminentă a legii), el presupune mai mult decât promovarea "abstractă" a violenţei. Într-adevăr, potrivit recomandărilor aprobate de Smith, acest criteriu necesită luarea în calcul a dimensiunii, probabilităţii şi iminenţei ameninţării (care trebuie analizate în raport cu „impactul unei investigaţii asupra vieţii private şi libertăţii de exprimare”)[63]. De aceea, deşi această reinterpretare nu mai impune necesitatea existenţei unor dovezi privind o "iminentă" încălcare a legii, ea se menţine în spiritul "standardului în materie de infracţionalitate".

Argumente în favoarea standardului în materie de infracţionalitate. Este mai uşor să se aducă argumente teoretice împotriva standardului în materie de infracţionalitate aplicabil în cazul investigaţiilor

din domeniul securității interne decât să se identifice un substitut. Standardul a fost adoptat după ce Comisia Church a documentat mai multe cazuri în care FBI-ul a desfăşurat investigații care au implicat atât utilizarea unui volum exagerat de resurse, cât şi amestecul nejustificat în activități politice care nu prezentau riscuri la adresa securității naționale. Această implicare excesivă, aşa cum a denumit-o Comisia Church, a reprezentat un argument în favoarea adoptării unui standard clar care să limiteze numărul investigațiilor la cele imperios necesare. Investigațiile necesare au fost definite ca fiind acelea care vizează acte infracționale însoțite de violență care au avut loc sau urmează să se producă.

Cazurile de implicare excesivă în investigațiile din domeniul securității naționale se încadrează în mai multe categorii. Probabil cele mai răsunătoare au fost cazurile în care, la solicitarea Casei Albe, FBI-ul a desfăşurat investigații cu privire la adversarii politici ai preşedintelui. Laurence Silberman, judecător şi fost ministru adjunct al justiției, a declarat în 1978 că "dintre toate abuzurile comise de diverse agenții guvernamentale în ultimii 20 de ani, cred că cel mai revoltător abuz a fost cel al preşedintelui Johnson, care a solicitat FBI-ului să încerce să găsească informații compromițătoare despre staff-ul senatorului Barry Goldwater, cu două săptămâni înainte de alegerile prezidențiale din 1964."[64] Există şi alte cazuri similare în care s-a apelat la FBI pentru discreditarea adversarilor politici din cadrul Congresului, a unor jurnalişti sau a altor persoane.

În multe alte cazuri, investigațiile au avut ca obiect grupări politice militante, cum ar fi:

- Grupări "de dreapta" sau "extremiste" angajate în "lupta anticomunistă";
- Grupări "anarhiste sau revoluționare";
- "Naționalişti de culoare" şi "extremişti";
- Grupări care promovează "supremația rasei albe";
- "Agitatorii" [65].

În aceste cazuri, deşi se pare că a existat o corelație între organizațiile investigate şi anumite acțiuni violente, sau legături cu servicii secrete străine, investigațiile desfăşurate au fost mult prea extinse în ceea ce priveşte numărul persoanelor şi grupărilor vizate, informațiile tangențiale culese despre acestea şi perioada de timp alocată acestor investigații lipsite de perspective. Informațiile tangențiale obținute au fost reținute în dosarele de anchetă şi, totodată, diseminate în cadrul guvernului; în felul acesta, administrația a putut utiliza în scopuri partizane informațiile despre activități politice legitime care au fost puse la dispoziția sa. [66]

Pornind de la concluziile Comisiei Church, este evident că excesele au fost facilitate de absența unor standarde precise în domeniul investigațiilor informative desfăşurate pe plan intern. Prin urmare, este uşor de înțeles de ce un standard în materie de infracționalitate reprezintă o soluție clară şi atractivă. Dacă acesta are un caracter prea restrictiv, trebuie

identificată o alternativă mai cuprinzătoare, care să nu mai permită însă repetarea abuzurilor din trecut.

Acest lucru nu se poate realiza rapid. Pentru a aborda situația într-o manieră responsabilă, trebuie să se stabilească, inițial, activitățile politice sau de altă natură desfăşurate pe plan intern pe care un guvern democratic este îndreptățit să le cunoască, astfel încât să fie în măsură să prevină eventualele amenințări. În SUA, legislația, deciziile executivului şi normele din domeniul informațiilor interne au fost concepute din perspectiva condițiilor ce trebuie îndeplinite anterior aplicării diferitelor tehnici de investigație. Pe de o parte, nu există prevederi oficiale cu privire la obiectivul activității de informații desfăşurate pe plan intern sau la tipul informațiilor care ar trebui să rezulte din această activitate. Numai existența unor astfel de prevederi va permite elaborarea unor norme care pun accent pe obiectivul activității de informații (ce tipuri de informații sunt necesare), în detrimentul mijloacelor utilizate (tehnicile de investigații utilizate).

Legislația canadiană, pe de altă parte, defineşte amenințările pe care trebuie să le gestioneze agenția care desfăşoară activități de informații pe plan intern, Serviciul Canadian de Informații privind Securitatea, (CSIS). CSIS este autorizat să culeagă informații despre activități "în legătură cu care există dovezi pertinente potrivit cărora acestea pot constitui o amenințare la adresa securității Canadei". Aceste activități sunt definite astfel:

- spionaj sau sabotaj, ori alte activități care vizează sau vin în sprijinul actelor de spionaj sau sabotaj;
- activități sub influență străină de natură să aducă atingere intereselor Canadei şi care sunt clandestine, au scop de dezinformare sau implică o amenințare la adresa unei persoane;
- activități care vizează sau vin în sprijinul amenințării sau al recurgerii la violență pentru atingerea unor scopuri politice;
- activități care vizează sau sunt menite să conducă la răsturnarea prin mijloace violente a guvernului canadian [67].

Chiar şi în condițiile unei definiri adecvate a obiectului activității de informații desfăşurate pe plan intern, se pune întrebarea dacă o anumită grupare constituie o amenințare sau are doar un discurs exacerbat şi care este volumul şi tipul probelor necesare pentru ca o grupare să fie considerată o amenințare ce trebuie avută în vedere. Fără a înțelege exact ce informații privind securitatea națională sunt necesare, este imposibil de apreciat dacă se justifică anumite restricții aplicabile mijloacelor de investigație.

Capitolul 7

DOUĂ PERSPECTIVE ASUPRA LUMII INFORMAȚIILOR

În precedentele cinci capitole am analizat cele patru elemente ale activității de informații - cele patru categorii de activități informative -, precum şi anumite aspecte privind relația dintre serviciile de informații pe de o parte şi celelalte structuri guvernamentale şi componente ale societății, pe de altă parte. Acum, vom aborda şi problema generală a naturii activității de informații în ansamblu, începând prin a face o comparație între aşa-numita "viziune tradițională asupra activității de informații" (care pune accentul pe obținerea, protejarea şi valorificarea informațiilor secrete cu relevanță în relațiile dintre națiuni) şi viziunea mai recentă, tipic americană, asupra activității de informații, care s-a conturat după cel de-al doilea război mondial.

Într-o anumită măsură, viziunea "tradițională" prezentată aici ne aparține. Deşi ea reflectă conceptele tradiționale ale activității de informații, aceste concepte nu au fost formulate de regulă în această manieră. (Trebuie reamintit faptul că, în trecut, nu s-au publicat multe lucrări pe tema activității de informații). Această viziune este utilizată aici ca termen de comparație menit să evidențieze caracteristicile viziunii americane care a apărut după cel de-al doilea război mondial.

Viziunea "tradițională" îşi are originea în una dintre cele mai vechi analize pe tema activității de informații, o carte clasică, *Arta Războiului,* scrisă de Sun Tzu, general şi strateg militar chinez din secolul 6 î.Hr. Iată cum a explicat el importanța activității de informații:

> Motivul pentru care prințul luminat şi generalul înțelept îşi învinge dușmanii de fiecare dată, iar izbânzile lor le depăşesc pe cele ale oamenilor de rând este previziunea.
> Ceea ce numim "previziune" nu este un dar al spiritelor sau al zeilor, nici nu rezultă prin analogie cu evenimente trecute sau în urma unor calcule. Ea poate fi obținută de la cei care cunosc situația inamicului (altfel spus, cei care au acces în tabăra inamicului).[1]

Spionajul este elementul principal al acestei viziuni asupra activității de informații. Dată fiind legătura strânsă dintre cunoaşterea secretelor dușmanului şi înfrângerea acestuia, este de la sine înțeles că protejarea propriilor secrete (contraspionajul) este la fel de importantă ca şi descoperirea secretelor adversarului. Sun Tzu identifică două metode de a obține acest rezultat:

- Atragerea agenților inamicului, prin lansarea unei oferte mai avantajoase;
- Trimiterea de spioni în tabăra inamicului, spioni care au fost induşi în eroare cu privire la propria lor situație, astfel încât, dacă sunt capturați şi forțați să vorbească, să-l poată înşela fără a fi ei înşişi conştienți de acest lucru[2].

Scopul fundamental al spionajului îl reprezintă o înțelegere foarte bună a strategiei inamicului, astfel încât planurile acestuia să poată fi dejucate, iar el să poată fi învins, cu cele mai mici pierderi posibile. Din punctul de vedere al lui Sun Tzu, pentru care este mai important să dejoci strategia inamicului decât să învingi pe câmpul de luptă, componenta informativă este la fel de importantă ca cea militară:

> De aceea, în război, cel mai important lucru este să dejoci strategia duşmanului, apoi să-i distrugi alianțele, pentru ca, în final, să-i ataci armata.[3]

Activitatea de informații este similară unui conflict armat, diferența constând în mijloacele utilizate.

Într-un articol care pledează pentru "dezvoltarea unui sistem de informații adecvat Statelor Unite", fostul director CIA, William Colby, face o distincție între un astfel de sistem şi sistemele de informații tradiționale, pe care le descrie astfel:

> Timp de secole, activitatea de informații a fost apanajul monarhilor şi generalilor. Spionajul guvernamental şi militar a scos la iveală secretele altor puteri, în scopul obținerii unor avantaje. Agenții secreți au uneltit pentru a-i discredita pe inamici ori pentru a-i sprijini pe adversarii lor [sic] din propria lor tabără. Spionul era prototipul acestei "discipline informative tradiționale."[4]

Colby defineşte "conceptul tradițional asupra activității de informații" ca fiind "un serviciu secret care descoperă un plan secret al duşmanului şi îl dezvăluie monarhului, cu scopul ca acesta să poată câştiga bătălia".[5] El susține că experiența acumulată de Statele Unite în perioada celui de-al doilea război mondial a dus la conturarea unei noi viziuni asupra activității de informații, care se deosebea, în privința unor aspecte fundamentale, de viziunea tradițională. În perioada postbelică, această viziune a continuat să capete contur, atât în rândul comunității de informații a SUA, cât şi în lumea academică. Acest capitol ia în discuție această nouă viziune şi face o comparație între aceasta şi viziunea "tradițională".

ISTORICUL VIZIUNII AMERICANE

Climatul instabil instaurat după izbucnirea celui de-al doilea război mondial şi după intrarea SUA în război, a dus la o sporire semnificativă a resurselor alocate de Statele Unite activităţii de informaţii. De asemenea, a condus la înfiinţarea unui serviciu central de informaţii (denumit iniţial Biroul de Coordonare a Informaţiilor şi, ulterior, Biroul de Servicii Strategice sau OSS), care avea ca obiective culegerea, analizarea şi centralizarea datelor şi informaţiilor privind securitatea naţională [6]. Deşi preşedintele Franklin Roosevelt a decis, în iulie 1941, înfiinţarea unui organism central care să centralizeze informaţiile, agenţia respectivă nu a fost înfiinţată până în decembrie 1941, atunci când neanticiparea atacului japonez de la Pearl Harbor a evidenţiat deficienţele în materie de analiză şi centralizare a numeroaselor informaţii fragmentare care erau disponibile.

Importanţa activităţii de analiză

OSS a înfiinţat un departament de cercetare şi analiză care urma "să analizeze toate informaţiile relevante, obţinute din surse deschise şi surse secrete"[7]. Deşi acest ideal nu a fost îndeplinit pe perioada celui de-al doilea război mondial, a fost, în cele din urmă, atins prin înfiinţarea Agenţiei Centrale de Informaţii, CIA, în 1947[8].

Acest accent pus pe analiza informaţiilor, pe corelarea şi centralizarea unor informaţii disparate în vederea conturării unei imagini cât mai corecte sugerează o viziune asupra activităţii de informaţii diferită de cea "tradiţională". Această nouă viziune acordă mai puţină atenţie confidenţialităţii, punând un accent deosebit pe funcţia analitică.

Această viziune a fost promovată cu succes, imediat după încheierea celui de-al doilea război mondial, de către Sherman Kent, fost ofiţer OSS şi viitor şef al Biroului pentru Estimări Naţionale al CIA, care, la vremea respectivă, avea ca sarcină întocmirea unor evaluări complete ale situaţiei internaţionale. Cunoscuta sa carte, *Informaţii strategice pentru politica externă a SUA*, pleda pentru înţelegerea activităţii de informaţii ca metodă ştiinţifică (în varianta sa de ştiinţă socială) aplicată problemelor strategice:

> Noi, cei de tradiţie liberală, considerăm că cercetarea este singurul proces care ne oferă adevărul sau ne apropie cel mai mult de adevăr. Insistăm – cum au făcut şi alte generaţii înaintea noastră - asupra faptului că adevărul trebuie obţinut printr-o cercetare bazată pe o metodă sistematică. Există o astfel de metodă în cadrul ştiinţelor sociale, care reprezintă, în linii mari, esenţa activităţii strategice de informaţii. Această metodă se aseamănă în mare măsură cu cea a ştiinţelor naturale. Nu este aceeaşi metodă, dar, fără îndoială, este o posibilă metodă de lucru.[9]

Desigur, activitatea de informaţii nu se poate reduce la metoda ştiinţelor sociale, chiar dacă aceasta reprezintă o componentă esenţială. La urma urmei, trebuie să existe date cărora să le poată fi aplicată. Deşi admite că anumite date trebuie obţinute prin mijloace clandestine, Kent susţine că viziunea tradiţională asupra activităţii de informaţii, care pune accent pe aspectul confidenţialităţii, este un mit. În opinia sa, analiza informaţiilor se poate baza pe informaţii nesecrete, din surse publice, la care se poate adăuga un număr redus de informaţii obţinute din surse secrete. Referitor la informaţiile necesare pentru elaborarea politicii externe – obiectul activităţii strategice de informaţii - el afirmă: "Unele dintre aceste informaţii pot fi obţinute prin mijloace clandestine, *însă marea lor majoritate trebuie obţinute prin activităţi de observare directă şi cercetare*".[10]

În forma sa extremă, această nouă viziune echivalează activitatea de informaţii cu un gen de ştiinţă socială, universală şi anticipativă. Această abordare a fost descrisă astfel de Colby în 1981:

> **Trebuie perfecţionată o nouă disciplină al cărei obiect specific de activitate îl reprezintă analiza informaţiilor**, iar procesul de cercetare şi dezvoltare a început deja. Această disciplină va merge mai departe decât analiza ştiinţifică, prin aplicarea unor noi tehnici de anticipare a unor evenimente probabile, în detrimentul explicării evenimentelor trecute. Experimentele specifice acestei noi discipline nu se limitează la comunitatea de informaţii, având loc, de asemenea, şi în centre de cercetări din domeniul ştiinţei informaţiilor, în mediul analiştilor care evaluează riscurile politice şi în cadrul previziunilor realizate de Clubul de la Roma, de studiul Global 2000 şi de alte studii.[11]

Importanţa analizei informaţiilor este o trăsătură definitorie a acestei noi viziuni asupra activităţii de informaţii. Pentru a înţelege mai bine această viziune, vom analiza argumentele pe care un adept al acesteia le va invoca pentru a-l convinge pe "tradiţionalist" de adevărul său. Se porneşte de la observaţia că, indiferent de viziunea asupra activităţii de informaţii, trebuie recunoscut rolul important al acesteia cel puţin în cazul câtorva tipuri de analize.

În primul rând, activitatea de culegere de informaţii generează imediat necesitatea analizei, fie tehnice (cum ar fi descifrarea mesajelor codificate), fie cu caracter general (cum ar fi compararea rapoartelor din două surse diferite pentru a verifica dacă informaţiile coincid sau se contrazic). Trebuie realizată o evaluare a informaţiilor primite pentru a stabili, de exemplu, dacă acestea trebuie acceptate ca fiind veridice sau dacă trebuie considerate ca o tentativă de dezinformare din partea adversarilor[12].

Adesea poate fi dificilă obţinerea directă a informaţiilor secrete relevante. În consecinţă, singura alternativă este să încerci să deduci respectivele informaţii pornind de la datele disponibile, cum ar fi

informațiile pe care adversarii nu le consideră ca fiind sensibile şi, de aceea, nu păstrează secretul asupra lor.

De exemplu, cel mai direct şi credibil avertisment privind iminența unui atac ar putea proveni de la un agent infiltrat în cartierul general al inamicului. În absența unui astfel de agent, trebuie să deduci intențiile inamicului din diferite frânturi de informații referitoare la desfăşurarea trupelor acestuia, la pregătirea pentru luptă a acestora sau la mobilizarea rezerviştilor. În plus, informațiile din surse publice pot fi, de asemenea, utile; de exemplu, înainte de atacul de la Pearl Harbor, Statele Unite erau interesate de locațiile şi itinerariile vaselor comerciale japoneze, considerând că, dacă japonezii ar fi intenționat să intre în război, ar fi luat măsuri în vederea retragerii flotei comerciale japoneze în ape sigure.

Până în acest punct, adepții viziunii tradiționale nu vor contesta necesitatea unor astfel de activități, în ciuda faptului că viziunea lor asupra activității de informații pune accentul, în primul rând, pe informațiile secrete. Apar semne de întrebare atunci când sfera activității de informații se extinde la nivelul „noii discipline a analizei informațiilor" promovată de Colby, o ştiință socială universală şi anticipativă, care acoperă toate aspectele vieții sociale.

Pentru o eficientă gestionare a problematicii militare şi a politicii externe, reprezentații unui guvern trebuie să dispună de mai multe informații despre potențialii lor adversari, şi nu doar de informații secrete de natură militară şi diplomatică. De asemenea, trebuie luați în considerare şi alți factori, cum ar fi situația economică a potențialului adversar, tendințele demografice, forțele politice interne. Referitor la aceşti factori, dificultatea nu constă atât în culegerea acestor date neprelucrate (deşi aceste aspecte pot constitui o provocare, în cazul unei societăți închise, cu un sistem politic totalitar), cât în evaluarea lor corectă.

De exemplu, în pofida caracterului deschis al procesului politic american, unui observator american sau de altă naționalitate i-ar fi greu să înțeleagă, cu atât mai mult să anticipeze deznodământul unei evenimente politic major, cum ar fi rezultatul unui vot în Congres sau alegerile prezidențiale. În mod cert, pentru o coordonare eficientă a politicii externe față de Statele Unite, o țară trebuie să fie conştientă de faptul că o bună înțelegere a acestor aspecte poate fi la fel de importantă ca şi obținerea unor informații secrete privind securitatea națională a SUA. Aşa cum a arătat Eliot Cohen, caracterul deschis al vieții politice americane din anii '30 nu a fost suficient pentru a le permite viitorilor adversari să o înțeleagă:

> Deşi Statele Unite erau accesibile agenților străini, atât celor oficiali, cât şi celor secreți, într-un anume sens, erau inaccesibile puterile Axei, datorită incapacității acestora de a înțelege modul în care funcționa un sistem democratic. Atât Germania cât şi Japonia au subestimat în nenumărate rânduri sistemul politic american, tenacitatea şi inventivitatea acestuia, dar şi capacitatea sa de a se organiza, de a

improviza şi de a produce rezultate. Aceste eşecuri majore pe linie de informaţii au dus la zdrobitoarea înfrângere a celor două state.[13]

În alte situaţii, informaţia care ar fi prezentat cel mai mare interes pentru o naţiune nu putea fi considerată o informaţie secretă deoarece, în momentul în care apărea necesitatea deţinerii acesteia, ea nici măcar nu exista încă. Sherman Kent exemplifică această situaţie prin problema cu care s-a confruntat Uniunea Sovietică atunci când a încercat să estimeze dacă Statele Unite intenţionau să se împotrivească invadării Coreei de Sud de către Coreea de Nord, în 1950. Dacă agenţii sovietici ar fi căutat în documentele americanilor dovezi privind decizia acestora de a se implica în conflict, nu ar fi găsit nimic, întrucât preşedintele Truman a luat decizia respectivă după ce invazia a început: "Astfel, dacă intenţiile unei persoane pot fi anticipate prin citirea documentelor sale personale, iar strategia poate fi stabilită pe baza informaţiilor aflate, situaţia de mai sus este un exemplu în care strategia este, prin definiţie, sortită eşecului."[14] Kent susţine că astfel de informaţii pot fi obţinute doar prin cercetare şi analiză:

> Am arătat că, dacă există informaţii cu privire la situaţia strategică (termenul folosit de Kent pentru a se referi la capacitatea militară, politică şi economică a unei naţiuni de a acţiona pe scena internaţională) a statului Great Frusina (o mare putere ipotetică, în viziunea lui Kent), la vulnerabilităţile acesteia şi la modul în care sunt percepute, precum şi informaţii despre situaţia şi vulnerabilităţile altor state implicate, atunci există posibilitatea de a anticipa *acţiunile pe care le-ar putea întreprinde*.
> Pentru ca previziunile să fie cât mai reale, sunt necesare alte două categorii de informaţii. Mai întâi, trebuie cunoscute acţiunile pe care Great Frusina le-a întreprins în trecut. În al doilea rând, trebuie cunoscut, în măsura posibilului, modul în care Great Frusina îşi estimează propria situaţie în circumstanţele date.[15]

Nu e nici o îndoială că astfel de informaţii şi raţionamentele care conduc la acestea constituie o parte vitală a gândirii strategice, în general, şi a politicii externe la nivel înalt, în particular. Nici o politică nu poate fi adoptată sau implementată fără a lua în considerare potenţialele acţiuni ale altor state. Cu toate acestea, nu este clar motivul pentru care aceste activităţi trebuie considerate "activităţi de informaţii secrete" şi trebuie să se desfăşoare în cadrul agenţiilor de informaţii[16]. Această problemă, care ridică întrebări importante privind relaţia dintre activitatea de informaţii şi factorii de decizie, a fost deja analizată în capitolul anterior.

Există două consecinţe ale viziunii netradiţionale asupra activităţii de informaţii; totodată, trebuie remarcat accentul pe care această viziune îl pune pe activitatea de analiză a informaţiilor. Prima consecinţă este că, în

mare parte, analiza strategică poate şi trebuie să se desfăşoare în cadrul agenţiilor de informaţii. Această activitate, în agenţiile de informaţii, este realizată conform unei metode ştiinţifice. Cu alte cuvinte, ştiinţele sociale pot sau ar trebui să furnizeze, în scopul cercetării, metode care să aibă atributele cercetării ştiinţifice. Conform acestei viziuni, pot fi obţinute rezultate mai bune în activitatea de informaţii, chiar dacă acestea nu reflectă neapărat date obţinute prin mijloace secrete, ci previziuni bazate pe fapte cunoscute de factorii de decizie. Astfel, este posibilă utilizarea informaţiilor secrete pentru evaluarea corectitudinii strategiilor.[17]

O a doua consecinţă este că analiza informaţiilor poate fi separată de procesul decizional, putând fi apolitică.[18] Ca urmare, s-a vorbit despre crearea, în cadrul comunităţii de informaţii, a unui departament analitic similar unui grup de reflecţie performant[19]. Din acest punct de vedere, activitatea de informaţii constituie, într-o mai mică măsură, un element de sprijin direct pentru factorii de decizie, reprezentând mai degrabă un fel de „enciclopedie" sau serviciu de documentare, de ale cărui informaţii ar trebui să beneficieze nu numai adversarii politici ai factorilor de decizie, ci şi opinia publică internă şi internaţională.[20] De exemplu, Colby anticipează o eră a liberului schimb în lumea informaţiilor, în care naţiunile recunosc "avantajele reciproce ale schimbului de informaţii, respectiv faptul că ambele părţi pot beneficia de pe urma angajamentelor de a nu ascunde faptul că deţin armament şi de a nu obstrucţiona mijloacele tehnice de verificare ale altor state, conform acordurilor privind controlul armamentelor." [21]

Oricât de neobişnuit poate părea acest lucru, potrivit acestei concepţii activitatea de informaţii reprezintă un demers similar ştiinţelor sociale, sau chiar echivalentul acestora.

Spionajul şi culegerea de informaţii prin mijloace tehnice

Indiferent de importanţa analizei în activitatea de informaţii, ca să fie analizate, datele brute trebuie să fie obţinute prin anumite mijloace. Deşi unele pot fi obţinute din surse deschise (presă, radio, televiziune), problema este că unele naţiuni nu fac publice nici măcar aspecte generale legate de forţele lor militare sau resursele economice alocate acestora. De aceea, chiar dacă viziunea lui Kent privind importanţa relativă a surselor deschise şi secrete ar fi reală în cazul majorităţii statelor, este clar că nu este valabilă în cazul statelor care ascund aproape toate datele referitoare la structura forţelor sale militare.

În special după cel de-al doilea război mondial, măsurile stricte de securitate întreprinse de fosta Uniune Sovietică au îngreunat activitatea de spionaj a SUA şi statelor occidentale menită să conducă la obţinerea datelor necunoscute despre forţele militare sovietice. Aşa cum am menţionat deja, problema s-a rezolvat în special datorită dezvoltării unor tehnologii sofisticate de survolare a teritoriului sovietic – mai întâi, avioanele U2, iar ulterior sateliţii de recunoaştere.

Aceste mijloace tehnice au reuşit să învingă măsurile de securitate sovietice şi, în acelaşi timp, au eliminat, se pare, alte riscuri specifice activităţii de spionaj. Problema determinării veridicităţii informaţiilor obţinute din surse umane a fost evitată prin utilizarea unor echipamente, care nu pot induce în eroare şi nu pot fi corupte. În acelaşi timp, accesul la o locaţie anume putea fi asigurat (deşi pentru a realiza fotografii clare, condiţiile meteo sunt vitale). Şi din acest punct de vedere, informaţiile obţinute prin mijloace tehnice (techint) par mai credibile decât cele obţinute din surse umane (humint).

Ca urmare, după cel de-al doilea război mondial, Statele Unite au acordat o importanţă exagerată informaţiilor techint în detrimentul informaţiilor humint. Acest lucru a făcut ca domeniul informaţiilor să fie considerat mai degrabă ştiinţific, nu doar pentru că utiliza cele mai noi şi sofisticate tehnologii, ci şi pentru faptul că incertitudinile aferente utilizării surselor umane puteau fi eliminate în mare măsură prin recurgerea la surse tehnice, care ofereau o vastă acoperire a teritoriului inamic şi permiteau observarea directă a evenimentelor. Rămâne de văzut dacă această dependenţă a Statelor Unite de sursele tehnice va continua în absenţa necesităţilor de informaţii care au stat la baza acesteia.[22]

Subestimarea contraspionajului

O altă caracteristică a acestei noi concepţii este tendinţa de a subestima importanţa contraspionajului, în general, a dezinformării şi contra-dezinformării. Acest lucru este în strânsă legătură cu noţiunea conform căreia activitatea de informaţii reprezintă o variantă a ştiinţelor sociale, care are ca obiect analizarea altor ţări. Deşi activitatea de informaţii diferă, în anumite privinţe, de ştiinţele socială, cele două discipline sunt similare, conform acestei viziuni.

De exemplu, Kent face observaţia că activitatea strategică de informaţii este, în terminologia propusă de el, o "extensie" în anumite sensuri, a efortului de cunoaştere, în general. Într-un anumit sens, există "obstacole dificile ridicate special, de către alte naţiuni" care creează impedimente. Cu toate acestea,

> oricât de importante ar fi, aceste extensii, aşa cum le-am denumit, nu au legătură directă cu esenţa problemei: activitatea de informaţii este acel simplu, firesc de a obţine informaţiile necesare derulării unor acţiuni de succes. Informaţiile strategice sunt acele informaţii pe care se bazează relaţiile noastre externe, pe timp de pace sau război.[23]

Pe de altă parte, din perspectiva "tradiţională", faptul că un adversar încearcă să păstreze confidenţialitatea unor informaţii vitale este chiar esenţa problemei: dacă adversarii nu încearcă să-şi ascundă intenţiile, atunci efectuarea unor analize complexe nu se impune.

Aceste puncte de vedere diferite privind importanța caracterului secret reflectă diferențele de opinii cu privire la informațiile secrete.[24] Dacă, potrivit viziunii "tradiționale", activitatea de informații este o componentă a confruntării propriu-zise cu adversarii, conform noii viziuni, activitatea de informații, ca orice știință, este un proces de descoperire a adevărului despre lume (natură), care poate fi denumit, doar în mod metaforic, luptă. Cu alte cuvinte, deși natura are secrete, acestea nu sunt protejate în mod deliberat, sunt, pur și simplu, adevăruri pe care nu le-am descoperit. Problema activității de informații nu constă atât în descoperirea intențiilor secrete ale inamicului (după cum a demonstrat-o războiul din Coreea, nici măcar adversarul nu poate ști cum va reacționa la viitoarele evenimente), cât în anticiparea comportamentului său, cu ajutorul metodelor științelor sociale. Acest lucru este valabil mai ales având în vedere faptul că analiza informațiilor pune un accent tot mai mare pe evaluarea tendințelor pe termen lung, care au, adesea, un caracter social și economic. În ceea ce privește situația socială și economică viitoare, nu pot fi obținute informații secrete, întrucât nici adversarul nu știe cu certitudine ce se va întâmpla, ce alternative va avea la dispoziție și cu ce circumstanțe se va confrunta.

Această tendință de a afirma că activitatea de contrainformații ocupă un loc marginal are impact asupra importanței acordate dezinformării și combaterii dezinformării. Considerând că activitatea de informații este similară unui demers din domeniul științelor sociale, noua viziune, ignoră, sau cel puțin minimalizează, posibilitatea dezinformării. Natura, deși își poate ascunde secretele față de oamenii de știință, nu încearcă, în realitate, să-i inducă în eroare.

Beneficiarii informațiilor

Cele două viziuni asupra activității de informații diferă, de asemenea, în ceea ce privește beneficiarii și utilizatorii informațiilor. Potrivit lui Colby, în concepția tradițională, șeful statutului este principalul și, probabil, singurul beneficiar al informațiilor. Această viziune se reflectă și în Legea privind securitatea națională din 1947, prin care a fost înființată Agenția Centrală de Informații, subordonată Consiliului Național de Securitate și președintelui, și nu Departamentului de Stat sau al Apărării. Consecința acestui mod de organizare a fost, se pare, faptul că CIA avea să rămână în strânsă legătură cu factorii de decizie de la nivel înalt și să monitorizeze și coordoneze, în numele acestora, activitatea celorlalte agenții de informații de la nivel departamental.

Întrucât noua viziune, susținută de foștii directori CIA, Colby și Turner, tinde să acorde o importanță mai mică informațiilor secrete, nu este surprinzător faptul că urmărește creșterea numărului beneficiarilor informațiilor. De exemplu, Turner are în vedere înființarea unei agenții internaționale de informații obținute prin satelit care să desfășoare activități de culegere de informații prin mijloace tehnice, în numele ONU, și să pună la dispoziția întregii lumi aceste informații.[25] De asemenea, Colby consideră

că suntem sau ar trebui să păşim într-o eră a liberului schimb de informaţii, în care volumul mare de informaţii, disponibil datorită tehnologiei moderne, oferă beneficii reciproce, nu unilaterale.[26] Această nouă eră trebuie să aibă la bază anumite principii, care „trebuie să insiste asupra beneficiilor reciproce ale schimbului liber de informaţii".

Activitatea de informaţii şi problemele etice

Poate părea ciudat să abordezi aspecte de ordin etic, atunci când discuţi un subiect ce vizează domeniul pragmatic al securităţii naţionale. Există riscul de a fi acuzat de naivitate. Cu toate acestea, cei care sunt preocupaţi de activitatea de informaţii s-au confruntat adesea cu problema moralităţii acesteia sau, mai precis, cu relaţia dificilă dintre aparenta imoralitate a demersurilor menite să-i convingă pe oameni să comită acte de trădare şi utilitatea, sau chiar necesitatea, acestui lucru.[27] În opinia lui Sun Tzu, în domeniul informaţiilor, cheia succesului o reprezintă capacitatea de a corupe persoane importante din tabăra inamicului. Sun Tzu apreciază că este vorba despre o problemă delicată, în special pentru cei care consideră că loialitatea este o adevărată virtute. În opinia sa, „influenţa morală", înţelegând prin aceasta „acea influenţă care îi determină pe oameni să fie de acord cu opiniile conducătorilor lor", este principalul element care determină victoria sau înfrângerea într-un război.[28] El pare, însă, conştient de faptul că necesitatea coruperii unor persoane de rang înalt şi a unor oameni de rând din alte ţări nu este în concordanţă cu idealul armoniei dintre supuşi şi conducătorii lor.

Chiar şi aşa, într-o manieră pe care o putem cataloga drept machiavelică, el îi îndeamnă pe cititorii săi să recurgă la spionaj, argumentând că cealaltă variantă – pe care, în opinia lui, cititorii ar considera-o mai „onorabilă" – este, de fapt, inumană. Având în vedere greaua povară pe care o presupune un război şi efectul nimicitor asupra vieţii oamenilor, pe un ton hotărât, el atrage atenţia:

> Cel care se luptă cu duşmanul său, de mulţi ani, pentru a obţine victoria într-o bătălie decisivă şi care, pentru că disprețuieşte rangul, onorurile şi aurul, rămâne în necunoştinţă de cauză cu privire la situaţia inamicului, este complet dezumanizat. Un astfel de om nu este general, nu îi este de nici un folos suveranului său, nu are şanse de izbândă.[29]

Faptul că Sun Tzu utilizează un argument de ordin etic, şi nu unul de ordin practic în favoarea spionajului, arată că el consideră necesar să îi determine pe cititori să îşi învingă scrupulele faţă de această metodă.

În pofida perioadei din care datează acest exemplu, problema moralităţii nu trebuie să fie privită ca o simplă curiozitate, având consecinţe de ordin practic în epoca modernă. De exemplu, în 1929, Secretarul de Stat Henry L. Stimson, la scurt timp după ce a fost numit de preşedintele Hoover,

a desfiinţat „Camera Neagră”, biroul criptografic al Departamentului de Stat, care timp de peste un deceniu a deschis corespondenţa diplomatică şi alte mesaje codificate. Se spune că gestul său a fost motivat de faptul că ”un gentleman nu citeşte corespondenţa altcuiva” [30]. Din punct de vedere al succesului repurtat de SUA în cel de-al război mondial, menţinerea facilităţilor criptografice în cadrul armatei şi al marinei militare a fost un lucru bun, care a deschis calea obţinerii unor victorii importante în timpul războiului, în urma spargerii codurilor diplomaţiei şi marinei japoneze.

Problema moralităţii activităţii de informaţii constă în faptul că aceasta este o formă clandestină şi duplicitară de luptă între naţiuni, spre deosebire de lupta armată, care este considerată, în mod tradiţional, ca fiind o confruntare mai deschisă (şi, prin urmare, mai onorabilă). Activitate de informaţii implică, în esenţă, dezinformarea şi depinde în mare măsură de influenţarea unor cetăţeni ai statelor inamice să comită acte de trădare. Aşa cum reiese din exemplul lui Stimson, acest gen de activitate nu corespunde optimismului manifestat de americani cu privire la moralitatea de care trebuie să dea dovadă relaţiile internaţionale. (Faptul că informaţiile obţinute prin interceptarea comunicaţiilor sunt considerate în prezent ca fiind „curate”, în comparaţie cu “imoralitatea” activităţii de spionaj, demonstrează măsura în care s-au redus standardele de moralitate aplicate la nivel internaţional) [31].

Viziunea lui Stimson şi-a pierdut valabilitatea în climatul politic instabil existent pe plan internaţional în anii '30, ca să nu mai vorbim de cel de-al doilea război mondial. Cu toate acestea, noua viziune asupra activităţii de informaţii, aşa cum a fost prezentată mai sus, are multe caracteristici care, în opinia susţinătorilor săi, o fac să pară mai morală decât cea “tradiţională”:

- Importanţa analizei (înţeleasă ca o ştiinţă şi având, astfel, prestigiul acesteia), în comparaţie cu activitatea de spionaj
- Primatul informaţiilor „curate” obţinute din surse tehnice asupra spionajului “imoral”
- Reducerea importanţei activităţii de contrainformaţii şi dezinformare, ceea ce atenuează percepţia negativă potrivit căreia activitatea de informaţii implică o confruntare între naţiuni
- Extinderea activităţii de informaţii spre alte domenii (schimbări sociale, evoluţii demografice, traficul de narcotice etc.) mai îndepărtate de esenţa politică şi militară a confruntării dintre naţiuni
- Diversificarea beneficiarilor informaţiilor, tendinţa care transformă o componentă secundară a sistemului politic (care este utilizată pentru promovarea intereselor naţionale, adesea în detrimentul altor state) într-un furnizor neutru de informaţii pentru guvern, opoziţie şi, în cele din urmă, pentru opinia publică naţională şi internaţională.

Prin urmare, această nouă concepţie asupra activităţii de informaţii poate fi înţeleasă ca o reafirmare a viziunii optimiste a SUA după realităţile dure ale relaţiilor internaţionale din timpul celui de-al doilea război mondial şi din primii ani ai Războiului Rece.

Capitolul 8

ELEMENTE PENTRU O TEORIE A CULEGERII INFORMAȚIILOR

Acest capitol reiterează întrebarea inițială: Ce sunt informațiile? Pe baza discuțiilor privind elementele de bază ale informațiilor, acum ne situăm pe o poziție superioară pentru a evalua diferitele concepții actuale referitoare la informații, în special pe cele prezentate în capitolul anterior drept "noua concepție americană" şi să încercăm să trasăm o definiție generală.

Termenul "informații" se utilizează cu referire la un anumit tip de informații, la activitatea de a obține informații de acest tip (şi obstrucționarea activității similare a altora), la organizațiile al căror rol este de a obține (sau a nega) aceste informații.[1] Din aceste trei categorii (informații, activitate şi organizație), prima este considerată de bază, în vreme ce următoarele două sunt definite prin termeni proprii. Astfel, prima problemă privind definirea informațiilor este de a stabili destinația acestora.

Sherman Kent dă o definiție pentru ceea ce el numeşte "informații externe pozitive la nivel înalt": adjectivele au rolul de a exclude informațiile care sunt de natură tactică sau operațională (nu "la nivel înalt"), informațiile interne (nu "externe") sau contrainformațiile (nu "pozitive"). Conform opiniei lui Kent, "Cunoştințele indispensabile pentru securitatea şi bunăstarea noastră nu sunt incluse. Sunt luate în discuție atât informațiile constructive cu care putem lucra pentru obținerea păcii şi libertății pe mapamond, cât şi informațiile necesare apărării şi intereselor țării noastre."[2]

În consecință, aceste informații sunt necesare în vederea derulării politicii externe şi luării hotărârilor majore privind evoluția şi dispunerea forțelor militare pe timp de pace. Conform opiniei lui Kent, strategia de securitate națională se poate baza pe informații.

Chiar din titlul cărții lui Kent (*Informațiile strategice pentru politica americană internațională*) rezultă că este vorba despre o dezbatere privind serviciile americane de informații şi mai puțin privind domeniul în sine. Drept urmare, definiția sa privind informațiile este formulată în conformitate cu cerințele guvernului american. Totuşi, nimic din definiția sau cartea sa nu pare a fi să limiteze aplicabilitatea acesteia numai la Statele Unite. Principiile de bază sunt de natură generală şi, într-adevăr, ținând cont de ceea ce se doreşte să se afle despre o țară străină, Kent nu vizează potențialii adversari ai Americii, ci inventează țara "Great Frusina" care serveşte drept țintă generală a serviciilor de informații. În această abordare, eu consider că afirmațiile lui Kent se aplică informațiilor în general.

După cum a arătat Kent (prin utilizarea adjectivelor "la nivel înalt", "extern" şi "pozitiv"), definiția pe care o dă tipurilor de informații nu este una exhaustivă. Trebuie avut în vedere, însă, ceea ce el numeşte "informații

tactice/operaţionale", "informaţii interne" şi "contrainformaţii". Cel mai important aspect este că descrierea lui Kent privind "informaţiile externe pozitive la nivel înalt" implică faptul că alte tipuri de informaţii nu sunt necesare pentru "securitatea şi bunăstarea noastră".

Se pare că definiţia lui Kent se concentrează numai pe solicitările de informaţii pe timp de pace. Pe timp de război, informaţiile ar trebui nu numai să ajute la luarea deciziilor militare de ordin strategic, ci şi la operaţiunile forţelor militare din teren. Totuşi, informaţiile tactice/operaţionale ar trebui incluse în orice discuţie generală despre informaţii şi este greu de crezut că Kent nu va fi de acord.

Situaţia poate fi diferită în ceea ce priveşte celelalte două restricţii. Prima, limitarea informaţiilor la subiecţi externi pare arbitrară, cel puţin în teorie. Ameninţările la adresa ţării şi intereselor sale pot fi atât interne cât şi externe sau pot implica grupări interne cu legături externe. După cum am văzut, definirea scopului informaţiilor interne reprezintă o sarcină extrem de dificilă.

Cu toate că, în general, vorbim despre securitate *naţională,* în aceste chestiuni un stat acţionează prin intermediul *guvernului* său*,* care de obicei consideră menţinerea formei sale de guvernământ drept un interes primordial. Observaţi că în definiţia de mai sus, Kent se referă la "apărarea Statelor Unite şi a *intereselor* sale". Acest enunţ demonstrează că democraţia americană ar putea fi pusă în pericol de ceva care nu a constituit o ameninţare de natură fizică. Indiferent de natura informaţiilor, informaţiile interne, necesare regimului pentru a se proteja împotriva schimbărilor revoluţionare sau violente, trebuie, de asemenea, să constituie o preocupare a serviciilor de informaţii. Desigur, subiecţii acestor informaţii şi cât importanţa conţinutului acestora depind, în mare măsură, de natura guvernului (regimului).

În plus, apărarea unui stat poate depinde de obstrucţionarea atât a acţiunilor serviciilor secrete ale statului inamic, cât şi a operaţiunilor militare ale acestuia; contrainformaţiile, de asemenea, informaţiile pozitive trebuie considerate ca fiind necesare pentru "apărarea ţării". Este mai puţin evident decât în exemplul anterior (informaţii tactice/operaţionale) faptul că Kent va fi de acord cu completările noastre.

În orice caz, domeniul informaţiilor trebuie extins pentru a putea include şi aceste secţiuni. Dat fiind că serviciile oferă informaţiile necesare pentru derularea strategiei de securitate naţională, trebuie să aibă în vedere şi furnizarea de informaţii care să justifice utilizarea forţelor militare pentru atingerea obiectivelor naţionale, precum şi furnizarea de informaţii care să contracareze activităţile de culegere de informaţii ale altor state. Totuşi, definiţia lui Kent privind informaţiile trebuie extinsă semnificativ dacă este vorba despre "informaţii indispensabile pentru securitatea şi bunăstarea unui stat".

Cu toate acestea, deşi trebuie să completăm definiţia lui Kent, adăugând informaţiile relevante pentru derularea strategiei de securitate naţională, în alte privinţe, definiţia este deja prea amplă. Un număr mare de

informaţii (de exemplu, informaţiile tehnice din domeniul fizicii şi ingineriei) pot fi necesare pentru luarea deciziilor privind anumite aspecte legate de dezvoltarea tehnologiilor militare, însă aceste informaţii, în mod obişnuit, nu vor putea fi considerate informaţii secrete. În mod similar, se impune o înţelegere generală a fenomenelor meteorologice în planificarea acţiunilor militare, dar acest tip de informaţii nu poate fi considerat de natură secretă.[3] Cu alte cuvinte, faptul că o anumită ramură a ştiinţelor naturii contribuie în mod semnificativ la îndeplinirea obiectivelor de securitate nu înseamnă că aceste informaţii dobândesc automat caracter secret.

Situaţia este mai puţin clară când vine vorba despre ştiinţele sociale. Activitatea de analiză specifică informaţiilor (de exemplu, situaţia politică dintr-o ţară străină şi prognosticul privind evoluţia acesteia) poate fi similară practicilor de evaluare din domeniul ştiinţelor sociale. Chiar şi aşa, cele două tipuri de analiză prezintă importante deosebiri care sugerează că pot fi necesare abordări diferite, deşi conţinutul este acelaşi.

Pentru a fi utilă, în evaluarea factorilor determinanţi ai contextului politici dintr-o ţară străină, analiza de informaţii trebuie să evidenţieze acele elemente care pot fi manipulate sau schimbate; de obicei, beneficiarul analizei este interesat, în cele din urmă, să influenţeze acea situaţie politică, nu numai să o cunoască. Pe de altă parte, o analiză ştiinţifică are ca scop să descopere cauzele fundamentale ale unei anumite situaţii, chiar dacă sau, mai ales, dacă sunt acestea nu pot fi schimbate. În măsura în care ştiinţele sociale pot anticipa desfăşurarea evenimentelor (conform lui Kent, acesta fiind motivul pentru care sunt utile în domeniul informaţiilor), acestea trebuie să considere viitorul ca fiind deja prestabilit. [4]

Totuşi, relaţia dintre informaţii şi ştiinţele sociale este complexă. Natura acestei relaţii se poate aborda mai bine în contextul altei diferenţe majore dintre informaţii şi ştiinţe – relaţia strânsă dintre informaţii şi natura lor secretă, pe de o parte, şi ştiinţa şi schimbul de idei, pe de altă parte.

Din punctul de vedere al viziunii tradiţionale asupra informaţiilor (să nu menţionăm percepţia populară a acestora) ceea ce lipseşte din definiţia informaţiilor este elementul care îi conferă caracterul secret. Pentru Kent, într-adevăr, preocuparea pentru caracterul secret al informaţiilor nu reprezintă o parte inerentă a acestora; deşi el observă că un inamic poate încerca să blocheze accesul altcuiva la informaţiile pe care acesta le solicită, el consideră că acest aspect este mai puţin important, asemănător problemelor organizatorice inerente structurii complexe a serviciilor secrete moderne:

> Indiferent de cât de importante sunt, aceste elemente complementare, după cum le-am numit (subtilitate, expertiză, *clandestinitate* şi mărime) sunt colaterale miezului problemei: activitatea de informaţii rămâne efortul cel mai simplu şi natural de a culege acele informaţii pe care se bazează derularea cu succes a unei acţiuni. [5]

Totuşi, legătura dintre informaţii şi caracterul secret este importantă pentru majoritatea acelora care fac distincţia între activitatea de informaţiile şi alte activităţi intelectuale. Reducând importanţa acestora, Kent îşi menţine poziţia conform căreia nu există o diferenţă elementară între activitatea de informaţii şi ştiinţele sociale; articolul lui Colby analizat mai devreme a condus la concluzia că, pe viitor, "Clubul de la Roma", să devină un model pentru serviciile de informaţii. [6]

Legătura dintre informaţii şi caracterul secret reflectă problema fundamentală a relaţiei dintre informaţii şi ştiinţă. Indiferent de similitudinile ce ar putea apărea, există o diferenţă elementară a obiectivelor celor două propuneri. Scopul ştiinţei îl constituie cunoaşterea, fie de dragul ştiinţei, fie pentru cunoaşterea şi mai aprofundată a naturii – abilitatea de a manipula forţele naturale conform voinţei omului în vederea obţinerii confortului, sănătăţii, longevităţii ş.a.m.d. Totuşi, conceptul privind lupta cu natura este numai o metaforă. De fapt, natura, deşi uneori este complicată şi dificil de înţeles, este indiferentă la eforturile umane şi nu acţionează premeditat ca să le obstrucţioneze.

Pe de altă parte, informaţiile implică o luptă reală cu inamicii omului, dusă pentru a câştiga unele avantaje în defavoarea altora. Prin urmare, nu este nici surprinzător şi nici lipsit de importanţă faptul că aceşti inamici adesea încearcă nu numai să împiedice eforturile cuiva de a-i cunoaşte, ci şi să dezinformeze şi să înşele. Eşecul informaţional al unei părţi poate fi succesul contra-informativ al celeilalte. Prin contrast, un succes informaţional al unei ţari reprezintă eşecul contra-informativ sau de securitate al inamicului acesteia.

Odată ce am înţeles că domeniul informaţiilor reprezintă o luptă între două ţări, înţelegem de ce contrainformaţiile nu sunt un element adiţional, ci parte integrantă a acestuia. Nu este suficient să limitezi sau să distorsionezi ceea ce adversarul poate afla despre tine ci şi să fii sigur de informaţiile culese despre un adversar fără ca acesta, prin resursele sale contra-informative, să te detecteze.

O obiecţie adusă acestei abordări este că ea ignoră rolul important pe care informaţiile din surse deschise îl pot juca în procesul culegerii de informaţii. Totuşi, această obiecţie se bazează pe o neînţelegere. Informaţiile obţinute din surse deschise sunt vitale atât pentru activitatea de informaţii, cât şi pentru ştiinţele sociale; potrivit viziunii tradiţionale asupra informaţiilor, sursele deschise reprezintă în primul rând o modalitate de a depăşi barierele care blochează accesul direct la informaţiile căutate. [7]

Culegerea de informaţii se bazează pe obţinerea accesului la informaţiile pe care cealaltă parte încearcă să le ascundă. Culegerea informaţiilor, în mod direct, înseamnă încălcarea barierelor de securitate pe care cealaltă parte le-a instituit pentru a-şi proteja informaţiile – prin interceptarea comunicaţiilor, sustragerea de documente, survolarea zonelor restricţionate şi fotografierea, mituirea oficialilor care au acces la informaţii, sau prin alte mijloace. Însă, în lipsa accesului direct la informaţii este posibil

ca acestea să fie deduse prin analiza altor date – obținute prin accesarea unor surse deschise, precum şi a altor date secrete.

În contextul acestei dezbateri, diferența dintre concepția lui Kent despre informații şi viziunea care pune accent pe caracterul secret este, în principal, o chestiune de percepție. Cea de-a doua concepție subliniază faptul că inamicul îşi protejează informațiile secrete, în timp ce Kent subliniază utilitatea informațiilor obținute din surse deschise. În anumită măsură, preocuparea lui Kent pentru sursele deschise reflectă opinia sa conform căreia sursele secrete nu sunt mereu de încredere. Este posibil ca un agent inamic să fie în realitate un agent dublu care dezinformează; poate este un impostor cu imaginație (care îşi atribuie o falsă calitate) şi care este suficient de inteligent să falsifice planuri de război verosimile pe care să le vândă la prețuri mari; este posibil că agentul să nu fie agent dublu, dar să fie deja compromis, astfel încât inamicul îl va aresta chiar în momentul în care transmite un mesaj important.

Deşi aceste fapte sunt adevărate, datele obținute din surse deschise pot fi manipulate cu scopul de a dezinforma. Să luăm de exemplu măsurile de dezinformare practicate de arabi, cu scopul de a-i convinge pe israelieni că nu va avea loc un atac în toamna anului 1973. Ei "au trecut de la a saluta inițiativele de pace ale lui domnului Kissinger din septembrie 1973 la a insera într-un ziar libanez ştiri referitoare la abandonarea şi deteriorarea echipamentelor militare din zona Canalului Suez." [8] Ideea este că orice tip de informații secrete pot deveni instrumente de dezinformare, iar analiza acestor informații trebuie să ia în considerare acest aspect. Într-adevăr, aceasta este diferența esențială între analiza informațiilor secrete şi ştiințele sociale: nu se falsifică rezultatele alegerilor cu scopul de a-l induce în eroare pe un sociolog care analizează aceste date (cineva ar putea, desigur, să facă acest lucru cu alte intenții). Analistul de informații nu este la fel de norocos. În cazul informațiilor secrete, chiar şi informațiile obținute din surse deschise nu sunt atât de inofensive precum par.

Din acest motiv, era informațională (în special, volumul mare de informațiilor din surse deschise aflate la dispoziția factorilor de decizie) nu afectează în mod substanțial această problemă. Deşi este important ca factorii decizionali să poată exploata eficient aceste surse de informații, ele nu trebuie să devină canale suplimentare de dezinformare. Într-adevăr, se poate spune că, dat fiind faptul că factorii decizionali s-au obişnuit să primească informări la minut din sursele deschise, a căror veridicitate nu este verificată şi să obțină informațiile direct, nefiltrate de către analiştii a căror sarcină este să le evalueze în ansamblu, posibilitatea de a fi dezinformați este mare.

Deşi Kent subapreciază semnificația surselor secrete, acesta se bazează pe considerente mai importante decât cele care stau la baza viziunii sale privind informațiile obținute din surse deschise. Spionajul se limitează, în mod evident, la obținerea informațiilor pe care inamicul le deține deja; nu poate anticipa comportamentul inamicului atâta vreme cât acesta nu a luat încă o decizie şi, prin urmare, nu ştie ce acțiuni să întreprindă. Pe de altă

parte, Kent consideră că această anticipare reprezintă este o sarcină informativă fezabilă, cu condiția ca serviciile să aplice metodele folosite de ştiinţele sociale. [9]

După cum consideră Kent, această metodă este nu numai utilă reprezentanților statului, ci şi obligatorie – cine nu o aplică poate fi acuzat că se bazează pe globul de cristal sau, să spunem mai politicos, pe intuiție:

> Atunci când beneficiarul ignoră evaluările serviciilor, bazându-se pe intuiția sa, el ar trebui să înțeleagă că refuză utilizarea a două instrumente pe care civilizația occidentală, începând de la Aristotel, le-a folosit pentru a-şi extinde orizontul său de cunoaştere – instrumentele fiind rațiunea şi metoda ştiințifică. [10]

Totuşi, indiferent cât de bine percepe situația politică un om de stat, se consideră ca fiind intuiție şi nu instrumente informaționale, respectiv "raționament şi metodă ştiințifică".

Dacă informațiile ar putea în mod pertinent să conducă la prognozele pe care le sugerează Kent în discursul său, factorii decizionali ar fi într-adevăr ridicoli să le ignore, iar sarcina lor ar fi mult mai uşoară. Optimismul lui Kent față de această abordare reflectă optimismul general al ştiinţelor sociale din anii 1940 şi 1950. Potrivit acestei concepții optimiste, adoptarea unei metode ştiințifice (precum diversele metode cantitative) şi a unei perspective ştiințifice (precum behaviorismul) vor permite ştiinţelor sociale o mai bună înțelegere a fenomenelor politice şi sociale (în cele din urmă şi cu acelaşi succes). În special, această percepție va fi destul de exactă pentru a sprijini funcția de prognoză pe care Kent o atribuie informațiilor.

În general, cercetarea în domeniul ştiinţelor sociale nu s-a materializat în ultimele decade, iar cercetătorii nu sunt foarte optimişti din acest punct de vedere. Capacitatea de anticipare a informațiilor nu va avea impactul pe care şi l-a imaginat Kent. Acest fapt ridică o întrebare mult mai dificilă în legătură cu relația adecvată dintre informații şi politică.

Toată lumea este de acord că informațiile se subordonează factorului politic, în sensul că activitățile de informații sunt menite a servi factorilor de decizie (deşi, după cum s-a observat, această subordonare va fi luată în discuție în măsura în care capacitatea de anticipare a informațiilor care se bazează pe ştiinţele sociale ar putea fi pusă în practică). Anvergura acestui serviciu poate fi accentuată. Pe de o parte, informațiile sunt uneori folosite ca un serviciu de referință, sursă de răspunsuri pentru anumite întrebări specifice. [11] Pe de altă parte, informațiile pregătesc analize vaste a problemelor importante, completate cu prognoze. În ambele cazuri, totuşi, informațiile ajută factorul politic care trebuie să ia deciziile.

Încrederea în aplicarea unei metode bazate pe ştiinţele sociale (dacă nu în prezent atunci în viitorul apropiat) care ar fi la fel de riguroasă şi avantajoasă precum metoda ştiințifică în ceea ce priveşte lumea materială arată că, în mod natural, experții merită să ia în seamă subiectele cu care

operează aceste metode. Totuşi, politica nu ar trebui să accepte numai informaţiile ca atare (dacă sunt disponibile fapte relevante, ar fi o nebunie să le ignorăm), ci şi evaluarea acestora.

Din păcate, asemenea metodă bazată pe ştiinţele sociale nu există. În acest caz, evaluările informaţiilor care încearcă să emită prognoze (în special prognoze contingente) nu diferă de concluziile pe care factorii decizionali le-ar putea trasa în situaţii similare. Alţi factori ar determina status-ul relativ care să garanteze cele două estimări.

Analistul de informaţii probabil are o pregătire mai mare în domeniu şi aproape cu siguranţă se poate aloca resurse considerabile acestei activităţi (precum disponibilitate şi accesul la date). Factorul politic probabil că ştie mai mult despre propriile sale politici de guvernare şi despre reacţiile diplomatice ale altor state faţă de acestea; este mult mai probabil să te concentrezi pe acţiuni fezabile pentru a influenţa situaţia; şi în orice situaţie, responsabil de rezultate. Cea mai cuprinzătoare şi relevantă evaluare a situaţiei din punct de vedere politic va rezulta din efortul comun al celor două grupuri.

Activitatea de informaţii are ca obiectiv culegerea de informaţii care să servească naţiunea pe care o reprezintă în competiţia cu celelalte. Prin urmare, aceasta are o natură dual㠖 indusă pe de o parte de faptul că se bazează pe informaţii, iar pe de altă parte de faptul că este o componentă importantă în cadrul conflictului dintre naţiuni (sau conflictul cu alţi adversari, cum ar fi grupările teroriste transnaţionale sau organizaţiile criminale). Prima componentă defineşte informaţiile secrete ca pe o ştiinţă socială cu caracter universal, care satisface nevoia de informaţii a factorilor politici despre alte ţări. În plus, asemenea noţiunilor ştiinţifice, informaţiile secrete de acest tip ar putea fi făcute publice, păstrându-şi caracterul secret.

A doua componentă, cea privind competiţia dintre naţiuni, ne conduce în altă direcţie. Dat fiind faptul că informaţiile secrete devin un instrument al competiţiei, dificultatea de a le înţelegere nu se datorează problemei în cauză; cele mai importante obstacole, respectiv cele care ar putea fi cele mai periculoase, sunt opera inamicului, care fie neagă informaţii, fie dezinformează deliberat. Totuşi, nu contează ce informaţii cauţi, trebuie să ţii cont şi de serviciile secrete inamice; într-adevăr, aceste servicii devin principala ţintă a activităţii de informaţii întrucât capacitatea de a le penetra şi, în cel mai fericit caz, a le manipula poate fi un succes răsunător. În acest sens, informaţiile au o dinamică internă care tinde să le transforme într-un duel al contrainformaţiilor, în care serviciul secret al fiecărei ţări, în majoritatea situaţiilor, caută să penetreze şi să manipuleze serviciul secret inamic.

În memoriile sale, fostul director CIA Colby critică modul în care James J. Angleton, şeful al contraspionajului din CIA pentru o perioadă lungă, a coordonat operaţiunile din departamentul său: "Într-adevăr, se pare că acordăm o atenţie mai mare KGB ca inamic al CIA decât Uniunii Sovietice ca inamic al Statelor Unite" [12] În mod evident, un serviciu secret are menirea să servească interesele naţiunii sale în contextul competiţiei

dintre națiuni. Însă, pentru a realiza acest lucru, de cele mai multe ori trebuie să se concentreze în special pe activitatea serviciilor secrete inamice.

Când un serviciu secret se axează în principal pe activitățile serviciului secret inamic (şi posibilitatea ca serviciul inamic să fie implicat în operațiuni de dezinformare), se expune riscului de a deveni "o imagine răsturnată" în care nimeni nu poate avea încredere şi nimic nu este ceea ce pare. Dacă serviciul pune constant la îndoială veridicitatea tuturor probelor, nu poate avansa în înțelegerea lumii exterioare. Activitatea de informații secrete este similară situației în care fizicianul pune mai mult accent pe teorie, decât pe practică.

Dacă un serviciu de informații îşi ignoră inamicii, totuşi, se expune riscului de a fi dezinformat şi de a percepe în mod eronat lumea pe care încearcă să o cunoască. În probleme privind informațiile secrete, analiştii cu greu pot avea încredere deplină în veridicitatea surselor pe baza cărora fac evaluări şi trebuie să aibă în vedere şi posibilitatea că acestea să fie eronate.

Aşadar, activitatea de informații are un caracter dual. Serviciile vor să afle tot ce se poate despre lume, iar obiectivul acestora poate fi caracterizat de versetul biblic pe care Allen Dulles, directorul CIA pe perioada mandatului preşedintelui Eisenhower, l-a adoptat ca motto: "Trebuie să cunoşti adevărul, iar adevărul te va elibera."[13] Însă, serviciile secrete niciodată nu trebuie să uite că aflarea adevărului implică o luptă cu un dușman care la rândul lui reacționează – sau adevărul nu reprezintă un obiectiv, ci un instrument în obținerea victoriei.

NOTE

INTRODUCERE

1. Activitatea lui Sherman Kent, fost ofiţer de informaţii, a anticipat această şcoală de gândire de la sfârşitul anilor 1940 şi rămâne cel mai cunoscut şi mai important reprezentant al acesteia. Subiectul a fost pentru prima dată expus în cartea sa Strategic Intelligence for American World Policy (Princeton, N.J.: Princeton University Press, 1949; republicată, 1966) şi este discutat în detaliu în capitolul 7 al acestei cărţi. A se vedea de asemenea lucrarea lui Bruce D. Berkowitz şi Allan E.Goodman, Strategic Intelligence for American National Security (Princeton, N.J.: Princeton University Press, 1989) care, conform autorilor, se dorea a fi o carte "scrisă în acelaşi spirit" asemeni celei scrise de Kent (deşi nu este o variantă "actualizată" a acesteia). Aceştia par să împărtăşească, cel puţin parţial, concepţia lui Kent referitoare la informaţiile strategice, argumentând că spre deosebire de informaţiile operaţionale, informaţiile strategice au "o bază mai mare şi un obiectiv mai amplu, incluzând economia, politica, studiile sociale şi studiul tehnologiei. Informaţiile strategice sunt concepute să ofere oficialilor o "perspectivă de ansamblu" şi prognoze pe termen lung de care au nevoie pentru a planifica operaţiunile viitoare" (4-5).

2. Senatorul David L. Boren, atunci preşedintele Comisiei Speciale pentru Informaţii, a precizat scopul reformelor propuse din domeniul informaţiilor de la începutul anilor 1990 pentru crearea unui "grup de experţi de talie mondială" – într-adevăr, "cel mai bun din lume". "Comunitatea de Informaţii: Cât este de importantă este?" Foreign Affaires 71, nr.3 (vara 1992): 61.

3. Una dintre primele şi cele mai cunoscute cărţi de acest tip începe cu următoarea afirmaţie "în prezent, există în Statele Unite, un cult puternic şi periculos – cultul informaţiilor". Publicitatea este o armă vitală în lupta împotriva "acestei fraternităţi secrete din aristocraţia politică americană": "Obiectivul acestei lucrări este să ofere cetăţenilor americani informaţiile interne de care au nevoie – şi la care au dreptul fără îndoială –să înţeleagă semnificaţia şi importanţa acestei probleme." Victor Marchetti şi John D.Marks, The CIA and the Cult of Intelligence (New York:Knopf, 1974), 4, 12.

4. Publicaţia britanică Informaţii şi Securitate Naţională a manifestat un interes deosebit pentru acest subiect, publicând numeroase studii istorice privind componenta istorică, militară şi diplomatică a activităţii de informaţii.

5. Un exemplu elocvent îl constituie lucrările lui David Wise. Comparaţi de exemplu, două dintre primele sale lucrări (scrise de Thomas B.Ross) – The Invisible Government (New York: Random House, 1967) şi The Espionage Establishment (New York:Random House, 1967) - cu încă două volume recente, The Spy Who Got Away: The Insight Story of Edward Lee Howard (New York: Random House, 1988) şi Mole Hunt: The Secret Search for Traitors that Shattered the CIA (New York: Random House, 1992). Titlurile în sine sugerează o schimbare de percepţie. Cea mai recentă carte a sa, Cassidy's Run:

The Secret Spy War Over Nerve Gas (New York: Random House, 2000) se axează pe un caz de spionaj, în acest caz, o operațiune cu un agent dublu care poate avea urmări neașteptate.

6. Aceasta explică numărul mare al exemplelor privind al doilea Război Mondial şi Războiul Rece; se cunosc mai multe aspecte legate de serviciile secrete din aceste perioade ale istoriei decât în alte perioade. Trebuie accentuat, totuşi, că aspectele pe care le ilustrează aceste exemple sunt considerate de interes general; relevanța acestora nu se supune anumitor situații de competiție între servicii.

7. O modalitate avantajoasă de a rămâne pe aceeaşi linie cu cea prezentată opiniei publice este de a vizita diferite siteuri web care conțin date privind serviciile secrete. Printre cele mai utile sunt siteurile web ale Federației Oamenilor de Știință americani (fas.org/irp); Muskingum College din Ohio (intellit.muskingum.edu/intellsite/maintoc.html) şi Loyola College din Maryland (***www.loyola.edu/dept/politics/intel.html)***.

8. Trebuie menționat că, înainte de a fi publicată, această lucrare a fost supusă analizei CIA şi Comisiei Speciale pentru Informații din Senatul american. Aceste două organizații au convenit că Războiul Tăcut nu conține informații clasificate.

CAPITOLUL 1: CE SUNT INFORMAȚIILE?

1. Lucrarea lui Sherman Kent, Strategic Intelligence for American World Policy (Princeton, NJ.: Princeton University Press, 1949; republicată, 1966) este alcătuită conform acestei descrieri a informațiilor în trei părți.

2. Herbert E. Meyer, Real-World Intelligence (New York: Weidenfeld şi Nicolson, 1987), 6. O scurtă bibliografie a lucrărilor de specialitate – informații de interes economic - poate fi găsită în lucrarea lui Robert David Steele, On Intelligence: Spies and Secrecy in an Open World (Fairfax, Va.: Comunicații Militare, 2000), 375-78.

3. Luați în considerare, de exemplu, eforturile depuse de administrația americană între anii 1991-92 de a alcătui o listă a "necesarului de informații" până în anul 2005. Impactul produs de terminarea Războiului Rece poate fi văzut într-o varietate mare de subiecte incluse. Pe lângă necesitățile privind informațiile tradiționale (precum planuri militare şi intenții diplomatice din țări importante), lista conținea solicitări de informații despre terorism internațional, proliferarea armelor de distrugere în masă, traficul de narcotice şi o serie de probleme de natură comercială şi economică. De asemenea, această listă cuprinde de asemenea solicitările factorilor politici pentru informații din aceste domenii neconvenționale precum noile tehnologii, demografia, migrația populației şi problemele medicale şi de mediu. A se vedea Loch K.Johnson, Smart Intelligence, Foreign Policy, nr.89 (iarna 1992.93): 60-61.

4. Pentru expunerea acestui subiect referitor la practica serviciilor secrete, vezi Adda Bozeman, Strategic Intelligence and Statecraft: Selected Essays (Washington, D.C.: Brassey s US, 1992).

5. Revelații la prăbușirea regimului comunist din Germania de Est. La momentul dispariției, serviciul secret al Germaniei Democrate a angajat peste 85.000 de persoane, a utilizat 500.000 de agenți și informatori part-time și a reținut dosarele a 6 milioane de cetățeni est-germani. După cum a arătat Jefferson Adams, "pentru un stat cu o populație de aproximativ 17 milioane de persoane, a reprezentat o rețea internă de o capacitate extraordinară". Werner Stiller și Jefferson Adams, "Prefață la Ediția din limba engleză", în Beyond the Wall: Memoirs of An Eat and West German Spy (Washington, D.C.: Brassey US, 1992), ix-x.

6. Cetățenii dintr-un stat democratic consideră aceasta ca fiind evidentă, dar recunoașterea că cineva poate fi un opozant al guvernului din acel moment, fără a fi inamicul unui regim sau al unei națiuni, reprezintă o realizare valoroasă care nu trebuie pusă la îndoială. Pe de altă parte, conceptul "Opoziție loială" implică posibilitatea unei opoziții care nu este. În vreme ce la nivel teoretic este clar, la nivel practic democrațiile liberale întâmpină dificultăți în a trasa o linie de demarcație. Pentru o retrospectivă a eforturilor guvernelor americane de a monitoriza și uneori de a distruge grupările și organizațiile considerate subversive, vezi Richard E. Morgan, Domestic Intelligence: Monitoring Dissent in America (Austin: Editura Universității din Texas, 1980), 15-87.

7. "Recomandările procurorului general privind infracțiunile, activitățile ilegale, investigațiile privind terorismul și securitatea internă", 1983, partea a III a. Recomandările sunt republicate în Camera Reprezentanților din SUA, Comisia Juridică, FBI Domestic Security Guidelines: Oversight Hearing, 98th Cong., prima sesiune, 1983.

8. Despre programul sovietic de achiziții militare, vezi Katherine A.S.Siblez, "Soviet Industrial Espionage against American Military Technology and the U.S. response, 1930-45", Intelligence and National Security 14, nr.2 (Vara 1999): 94-123 și Soviet Acquisition of Militarly Significant Western Technology: An Update (Washington, D.C.: Government Printing Office, 1985). Pentru o scurtă prezentare a programului sovietic de înarmare din anii 1970 și reacția SUA și a statelor aliate față de acesta, vezi Gus W.Weiss, "The Fairwell Dossier", Studies in Intelligence 39, nr.5 (1996): 121-26, disponibil la ***www.odci.gov/csi/studies/96unclass/farewell.htm***.

Se pare că serviciul rus de informații externe a continuat să culeagă informații secrete de natură tehnică și industrială de la alte țări. Centrul american de contrainformații (NACIC, organizație de colaborare între agenții care operează sub auspiciile Consiliului Național de Securitate) precizează, "Conform surselor media, președintele rus Boris Elțîn a confirmat la Moscova pe data de 7 februarie 1996 că Rusia este implicată în spionaj industrial, însă informațiile culese de agențiile secrete ruse nu sunt utilizate în mod eficient." NACIC, Counetrintelligence News and Developments, Martie 1966, 1, disponibil pe ***www.nacic.gov/cind/1996/mar96.htm***.

În ceea ce privește programul Chinei, vezi "Raportul Comisiei Cox": Raportul Comisiei Speciale pe probleme de securitate națională și amenințări de natură economică și militară din partea Chinei (Washington, D.C.: Government Printing Office, 1999) capitolul 1, disponibil pe ***www.house.gov/coxreport***.

9. Un fenomen separat, care nu vizează în mod direct problema sprijinului informaţional oferit factorului politic, îl constituie modalitatea prin care guvernul se foloseşte de informaţii pentru obţine bani. Un serviciu secret dispune de mai multe posibilităţi de a face bani, fie prin auto-finanţate, fie să fie prin finanţare guvernamentală. Operaţiunile clandestine ale unui serviciu pot fi folosite pentru a derula asemenea activităţi profitabile, precum traficul de droguri şi alte tipuri de contrabandă, iar în urma operaţiunilor clandestine se pot obţine informaţii din interior pentru speculaţii financiare. Nu este clar în ce măsură statele au folosit serviciile secrete în acest scop.

   Franţa reprezintă un astfel de exemplu care a devenit public. Conform fostului şef al serviciului francez de informaţii externe, acest serviciu a aflat în noiembrie 1971 că guvernul american a decis să diminueze valoarea aurului în luna următoare, deşi acest lucru a depreciat semnificativ dolarul. "Prin vânzarea tacită a dolarilor şi cumpărarea francilor pe o serie de pieţe financiare internaţionale, Banca centrală a Franţei a putut acumula un profit enorm – prin forţe proprii, suficient pentru a finanţa toate operaţiunile Serviciului". Contele de Marenches şi David A. Andelman, The Fourth World War (New York: Morrow, 1992), 114-15.

10. Datorită forţei sale tehnologice şi economice, Statele Unite s-au axat pe protecţia secretelor din aceste domenii. Din 1995, preşedintele a prezentat anual Congresului un raport privind spionajul extern care avea drept ţintă industria americană. Aceste rapoarte şi Legea Spionajului Economic din 1996, pot fi găsite pe site-ul Centrului naţional pentru contrainformaţii, ***www.nacic.gov***.

   Alte surse numără General Accounting Office, Economic Espionage: Information on Threat from U.S. Allies (GAO/T-NSIAD-96-114), disponibil pe ***www.nsi.org/Library/Espionage/allies.txt***, şi Peter Schweizer, "The Growth of Economic Espionage: America is Target Number One", Foreign Affaires 75, nr. 1 (Ianuarie-Februarie, 1996): 9-14.

11. Restricţiile pe care şi le-au impus Statele Unite în ceea ce priveşte utilizarea informaţiilor de natură economică nu au oprit acuzaţiile altor state, după cum este ilustrat de controversa din jurul sistemului "Echelon" de culegere de date din comunicaţiile internaţionale. "Echealon" se referă la un sistem automat de selectare printr-o cantitate imensă de date interceptate prin diferite metode de către Statele Unite şi aliaţii acestora a căror limbă oficială este engleza. În februarie 2000, un raport oarecum fantezist pregătit pentru Parlamentul European acuza Statele Unite şi pe aliaţii lor că au folosit informaţiile obţinute prin acest sistem pentru a-şi ajuta companiile să câştige avantaje comerciale. Duncan Campell, Interception Capabilities 2000, Raportul pentru Directorul General pentru Cercetare din Parlamentul European (Departamentul Programe de Evaluare a Opţiunilor Tehnice şi Ştiinţifice) disponibil pe ***www.iptvreports.mcmail.com/ic2kreport.htm#Report***.

   Aceste acuzaţii au fost negate de către fostul director al CIA, James Woolsey, într-o conferinţă de presă pe data de 7 martie, 2000. Woolsey a pretins că informaţiile care vizau corporaţiile străine erau limitate la 3 domenii: aplicarea sancţiunilor, vânzarea echipamentelor militare şi produselor utilizate în producerea armelor de distrugere în masă şi depistarea încercărilor de mituire de către corporaţiile non-americane în competiţie cu cele americane. Woolsey a precizat că situaţiile menţionate de Campbell se refereau la încercările corporaţiilor străine de a câştiga comenzile de export prin mituirea oficialilor statului care achiziţiona. Informarea Centrului de Presă, "Intelligence

Gathering and Democracies: The Issue of Economic and Industrial Espionage", ***www.fpc.gov/wool0300.htm***.

12. Conform unui studiu pe această temă, "Statele Unite deţin un arsenal tehnic impresionant de monitorizare pe arii întinse de pe pământ, oceane şi atmosferă în scopul asigurării securităţii naţionale. Aceste sisteme au cules date sofisticate care se întind pe zeci de ani şi care constituie o arhivă istorică unică. De asemenea, aceste sisteme pot fi utilizate pentru monitorizarea mediului." Scott Pace, Kevin M.O Conell, şi Beth E. Lachman, Using Intelligence Data for Environmental Needs: Balancing National Interests, MR-799-CMS (Santa Monica, California:RAND, 1997), 2.
13. Despre posibilele implicaţii ale erei informaţionale asupra serviciile secrete şi a activităţii de informaţii, vezi Bruce D.Berkowitz şi Allan E.Goodman, Best Truth: Intelligence in the Information Age (New Haven, Conn.:Yale University Press, 2000).
14. Comisia Guvernamentală a SUA pentru politică externă (Comisia Murphy), Report (Washington DC, Government Printing Office, 1975), 100.
15. Vezi John Ranelagh, The Agency: The Rise and Decline of the CIA (New York: Simon şi Schuster, 1986), 199-200, pentru analiza conflictelor de la sfârşitul anilor 1940 şi începutul anilor 1950, între Biroul pentru Coordonarea Politicilor (agenţia guvernului SUA pentru acţiuni secrete) şi Biroul de Operaţiuni Speciale (departamentul de spionaj al CIA). Vezi Cristopher Andrew, Her Majesty's Secret Service: The Making of the British Intelligence Community (New York: Viking, 1986), 476-77, pentru informaţii privind rivalitatea dintre Serviciul Secret al Marii Britanii şi Departamentul de Operaţiuni Speciale care a fost înfiinţat, aşa cum spunea primul ministru Winston Churchill, pentru a „pune Europa pe jar" (adică, derularea de activităţi de sabotaj într-o Europă ocupată de naziştii în timpul celui de-al Doilea Război Mondial şi pentru susţinerea forţelor partizane care se opuneau ocupaţiei germane).

CAPITOLUL 2: SPIONI, MAŞINI ŞI BIBLIOTECI: CULEGEREA DE INFORMAŢII

1. Această clasificare cuprinde cele mai utilizate metode de culegere de informaţii, dar nu este completă. De exemplu, informaţiile secrete pot fi procurate şi prin furtul de documente sau coduri de la ambasada adversarului. Acest furt poate fi considerat HUMINT, dar diferă de spionaj, aşa cum este el descris aici.
2. Din nefericire, termenul de „agent", frecvent utilizat, este ambiguu: se referă în general la sursă, deşi uneori se referă la un ofiţer de informaţii, aşa cum este menţionat în lexiconul Biroului Federal de Investigaţii al SUA (FBI).
3. Pentru a simplifica, această analiză se referă la ofiţeri de informaţii însărcinaţi cu spionarea ţărilor în care se află la post. Nu este neapărat vorba despre asta, ofiţerii se pot afla la post în *Freedonia* pentru a recruta *reuritani* (din serviciile secrete străine, din serviciile de informaţii sau din instituţiile militare) care sunt şi ei aflaţi la post acolo. În acest caz, ofiţerii pot fi denunţaţi (apartenenţa lor la un

serviciu de informaţi poate fi divulgată) autorităţilor *freedoniene*, scopul acoperirii lor fiind să evite suspiciunile *reuritanilor*. De asemenea, ofiţerii de informaţii pot lucra în propria ţară pentru a recruta diplomaţii străini aflaţi acolo.

4. În alte dicţionare de informaţii (cum este acela al fostei Uniuni Sovietice), o deosebire comparabilă între ofiţerii „legali" şi „ilegali" ia locul acoperirii oficiale/acoperirii neoficiale (NOC). Referirea nu priveşte legalitatea prezenţei ofiţerului în ţara gazdă, ci mijloacele prin care el comunică cu sediul său central. Un ofiţer ilegal este cel care comunică direct cu sediul său central, fără a menţine contactul cu instituţiile „legale" din ţara gazdă (ambasada, consulatul, oficiul de comerţ şi altele). În acest fel, un ofiţer „ilegal" este asemănător cu un ofiţer aflat sub acoperire neoficială (NOC).

5. În mod paradoxal, în unele cazuri, supravegherea personalului unei ambasade străine şi a străinilor în general de către serviciul secret al unei ţări străine este atât de strictă încât singura modalitate sigură de a comunica cu o sursă din guvernul acelei ţări este ca un ofiţer de informaţii care lucrează sub acoperire diplomatică să-l contacteze într-o manieră relativ „deschisă". De exemplu, în cazul lui Oleg Penkovsky, un colonel în serviciul secret al armatei sovietice (GRU) care a lucrat pentru serviciile de informaţii americane şi britanice la începutul anilor '60, o problemă importantă a operaţiunii a fost cum să fie contactat în Moscova, unde supravegherea serviciilor de contra-informaţii sovietice făcea foarte dificilă orice încercare de a-l întâlni sau comunica cu el clandestin. Una din soluţii a fost să se profite de faptul că întâlnirile cu diferiţi diplomaţi americani şi britanici făceau parte din rutina muncii lui Penkovsky în domeniul ştiinţei şi tehnologiei. Un ofiţer de informaţii se putea da drept un astfel de diplomat, urmând să folosească un semn prestabilit (cum ar fi să poarte un ac de cravată cu pietre roşii) pentru ca Penkovsky să-l recunoască. După ce identifica persoana de contact în îndeplinirea unei activităţi diplomatice de rutină, lui Penkovsky urma să i se spună: *mergi la toaletă, să spunem, şi [diplomatul/ofiţerul de informaţii] te urmează după cinci minute şi îţi preia mesajul. Nu este necesar să aibă loc vreo discuţie personală sau altceva de acest fel. [Astfel de întâlniri sunt]... sigure pentru că în două sau trei minute materialul se află în mâini sigure şi afacerea este terminată. Nu este necesar să călătoreşti... Aceasta este metoda cea mai sigură*.

   Din nefericire, alte metode mai nesigure erau folosite mai des şi s-a sugerat că acestea au contribuit la identificarea lui Penkovsky ca informator, la arestarea şi executarea lui ulterioară. Vezi Jerrod L. Schecter şi Peter S. Deriabin, *The Spy Who Saved the World* (New York: Scribner, 1992), 98, 287-99, 314-15, 409-11.

6. Pentru ca această funcţie de „căsuţă poştală" să funcţioneze, trebuie să se înţeleagă că, deşi acest lucru nu este recunoscut oficial, o ambasadă sau o instituţie diplomatică are în rândul personalului său oameni capabili să lucreze cu informaţii de importanţă deosebită sau secrete din surse voluntare. Un exemplu al caracterului cvasi-public al acestui tip de activitate secretă este dat de Allen Dulles, fostul director al CIA. După câte spune Dulles, curând după ce a fost trimis ca ofiţer de informaţii în Elveţia, în timpul celui de-al Doilea Război Mondial, un ziar elveţian important a publicat un articol în care îl descria ca trimisul special şi secret al preşedintelui Roosvelt. Dulles comenta că „neoficial, cineva ar fi putut crede că această publicitate nedorită ar fi putut să-mi pună piedici. Ce s-a întâmplat a fost exact invers... Ca rezultat [al

articolului], rețeaua mea a adunat o mulțime de informatori, unii excentrici, e adevărat, dar și unii extrem de valoroși." Allen Dulles, *The Craft of Intelligence* (New York: Harper și Row, 1963), 7.

Puteți citi despre unul dintre cei mai valoroși agenți pentru care Dulles a jucat rolul de „căsuță poștală" în nota 17.

7. Operațiunea sub acoperire poartă diverse denumiri, de exemplu: „post" (în jargonul american) și „rezidență" (*rezidentura* în jargonul sovietic și rus).

8. Problemele care apar odată cu angajarea unor cetățeni ai țării gazdă în ambasade sunt binecunoscute. Scriind despre perioada în care a ocupat funcția de ambasador al SUA la St. Petersburg, Rusia, la începutul anilor 1830, James Buchanan remarca: „suntem mereu înconjurați de spioni mai mari sau mai mici. Nu prea poți să angajezi un servitor care nu este agent secret al poliției." *Mission to Russia* (New York: Arno, 1970), 339.

   Pentru o descriere jurnalistică mai recentă a problemelor de securitate ridicate de folosirea excesivă a angajaților cetățeni ai țării gazdă în ambasade, vezi Ronald Kessler, *Moscow Station: How the KGB Penetrated the American Embassy* (New York: Scribner, 1989).

9. De exemplu, ocuparea ambasadei SUA la Teheran în noiembrie 1979 (și sechestrarea personalului ambasadei) părea că a sistat complet culegerea de informații din surse umane în Iran de către Statele Unite. Când a început planificarea acțiunii militare de salvare a ostaticilor, nu era „niciun agent american pe teren" și CIA a fost forțată să infiltreze un agent în Iran pentru a ajuta la culegerea informațiilor necesare pentru a planifica acțiunea de salvare. Charlie A. Beckwith și Donald Knox, *Delta Force: The U.S. Counter-Terrorist Unit and the Iran Hostage Rescue Mission* (New York: Harcourt Brace Jovanovich, 1983), 196-97, 220-21.

10. Acoperirea poate fi și o afacere inițiată, deținută și condusă chiar de serviciul de informații, o astfel de organizație fiind cunoscută ca aparținând serviciilor de informații (*proprietary*). O organizație de acest tip poate fi utilă pentru activități secrete, precum și pentru a oferi acoperire ofițerilor de informații. De exemplu, o afacere în domeniul transporturilor poate să faciliteze transportul clandestin de arme și provizii pentru rebeli.

11. La începutul anului 1941, Sorge a raportat că Germania intenționa să încalce pactul de neagresiune cu Uniunea Sovietică și să o atace în iunie. Rapoartele sale privind intenția lui Hitler de a încălca acordul și data precisă referitoare la începerea ofensivei germane au fost ignorate de Stalin. Dictatorul sovietic era aparent convins că acestea și alte informații despre duplicitatea germană fuseseră fabricate de britanici pentru a provoca o ruptură între Germania și Uniunea Sovietică și pentru a împinge Moscova într-o alianță cu Londra. Se pare că Stalin a considerat rapoartele lui Sorge asupra intențiilor japoneze mai credibile, parțial deoarece corespundeau cu mesajele japoneze interceptate de sovietici. Pentru relatări despre viața și activitatea lui Sorge ca ofițer de informații sovietic, vezi Gordon W. Prange, cu Donald Goldstein și Katherine V. Dillon, *Target Tokio: The Story of the Sorge Spy Ring* (New York: McGraw-Hill, 1984)

12. Pentru relatări despre viața și activitatea lui Cohen ca agent israelian, vezi Stanley A. Blumberg și Gwinn Owens, *The Survival Factor: Israeli*

Intelligence from World War I to the Present (New York: Putnam, 1981), 208-24.

13. Această relatare se bazează pe cartea lui John Barron, *KGB Today: The Hidden Hand* (New York, Reader's Digest, 1983; New York: Berkley, 1985), 247-314.

14. Dintre membrii blocului sovietic, Germania de Est a fost în mod special adepta plasării de ofițeri cu acoperire neoficială (NOC) (sau, pentru a folosi termenul sovietic, „ilegali") în vest, în special în Germania de Vest, ținta ei principală. Folosirea ofițerilor ilegali a fost parțial impusă Germaniei de Est deoarece eşecul din prima parte a Războiului Rece de a dobândi recunoaştere diplomatică însemna că aceasta nu avea ambasade şi consulate în multe din țările non-comuniste. Utilizarea ofițerilor ilegali a fost facilitată şi de faptul că Germania de Vest a încurajat activ imigrarea din Est. Conform declarațiilor unui fost ofițer de informații est-german, între două şi trei mii de agenți erau la post până la sfârşitul anilor '50. Cel mai faimos a fost Guenther Guillaume care a penetrat cu succes elita politică vest-germană, devenind secretarul personal al cancelarului Willy Brandt. El a ocupat această funcție între 1969 şi 1974, când a fost arestat. Cristopher Andrew şi Oleg Gordievsky, *KGB: The Inside Story* (New York: HarperCollins, 1990; ediția HarperPerennial, 1991), 448-50. Pentru descriere a utilizării de către Germania de Est a ofițerilor ilegali, din perspectiva unui fost ofițer de informații est-german, vezi Werner Stiller cu Jefferson Adams, *Beyond the Wall: Memoirs of an East and West German Spy* (Washington D.C.: Brassey's [U.S.], 1992), 41-118, passim.

15. Pentru o trecere în revistă a activităților HUMINT ale Chinei, vezi Nicholas Eftimiades, *Chinese Intelligence Operations* (Arlington, Va.: Newcomb, 1998), cap.5, 28-44. Referitor la programul Chinei în vederea obținerii de tehnologie performantă din SUA, vezi „Cox Committee Report": *Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China* (Washington DC: Government Printing Office, 1999), cap.1, disponibil la www.house.gov/coxreport. Vezi şi „China's High-Tech Espionage", o evaluare în două părți a *Sources and Techniques of Obtaining National Defense Science and Technology Intelligence*, un „manual" de origine chineză despre spionajul în vest, la Centrul Național de Contra-informații [în continuare numit NACIC], *Counterintelligence News and Developments* (iunie şi septembrie 2000), vol. 2 şi 3. Aceste evaluări pot fi găsite la www.nacic.gov, website-ul NACIC.

16. Totuşi, nu poate fi exclusă posibilitatea ca, după ce a fost abordată de un ofițer de informații străin, sursa să raporteze încercarea de recrutare propriului guvern şi să fie instruită „ să coopereze".

17. Vezi Joseph E. Persico, *Piercing the Reich: The Penetration of Nazi Germany by American Secret Agents during World War II* (New York: Viking, 1979), 62-72, 328.

18. Atât Burgess şi Maclean au lucrat pentru Ministerul de Externe, în timp ce Philby a intrat în serviciul de informații britanic (MI6) şi a ajuns şeful direcției de contra-informații şi ofițerul de legătură din Washington cu CIA şi FBI. Vezi Andrew Boyle, *The Fourth Man* (New York: Dial, 1979) pentru informații privind rețeaua de spionaj sovietică care s-a format în 1930 la Universitatea Cambridge. Vezi şi Robert Cecil, "The Cambridge Comintern", în *The Missing Dimension: Governments and Intelligence Communities in the Twentieh*

Century, ed. Cristopher Andrew şi David Dilks (Urbana: University of Illinois Press, 1984).

19. Serviciul de Securitate al Apărării, Centrul de Studii de Securitate, *Recent Espionage Cases*, 1975-1999 (septembrie 1999), disponibil pe www.dss.mil/training/pub.htm, conţine o descriere şi rezumate ale cazurilor recente. Theodore R. Sarbin, Ralph M. Carney şi Carson Eoyang analizează diversele motivaţii ale implicării în activitatea de spionaj în *Citizen Espionage: Studies in Trust and Betrayal* (Westport, Conn.: Praeger, 1994).
20. David Wise, *The Spy Who Got Away: The Inside Story of Edward Lee Howard* (New York: Random House, 1998).
21. Vezi Mary S. Lowell, *Cast No Shadow: The Life of the American Spy Who Changed the Course of World War II* (New York: Pantheon, 1992).
22. Pentru o descriere a afacerii Dejean, vezi John Barron, *KGB: The Secret Work of Soviet Secret Agents* (New York: Reader's Digest, 1974), 114-40.
23. Allan Dulles, *The Craft of Intelligence* (Boulder, Colo.: Westview, 1985), 216.
24. Dacă spionul capturat refuză să coopereze, se poate ca serviciul de informaţii care l-a capturat să acţioneze în numele lui, trimiţând mesaje din partea sa. O astfel de substituire poate funcţiona în situaţii cum este spionajul în timp de război pe teritoriu inamic, când nu este de aşteptat ca sursa să se întâlnească faţă-n faţă cu angajatorii săi.
25. Cristopher Andrew, *Her Majesty's Secret Service: The Making of the British Intelligence Community* (New York: Viking, 1986), 488. Pentru o relatare privind "*The Double Cross System*" scrisă de cel care a coordonat acest sistem, vezi J.C. Masterman, *The Double Cross System in the War of 1939 to 1945* (New Heaven, Conn.: Yale University Press, 1972).
26. Un manual de pregătire vechi şi totuşi interesant, conceput de serviciile de informaţii ale armatei sovietice, conţine lecţii despre comunicarea şi controlul surselor de informaţii din Statele Unite. Acesta a fost unul din materialele furnizate de Oleg Penkovsky, un ofiţer militar sovietic care a spionat pentru Statele Unite şi Marea Britanie la sfârşitul anilor '50, începutul anilor '60. "The Prikhodko Lecture" în *The Penkovsky Papers*, ed. Frank Gibeny (New York: Doubleday, 1965), 102-62.
27. Wise, *The Spy Who Got Away*, 198-205. Pentru ca trucul să fie complet, la întoarcerea acasă, soţia lui Howard a sunat la biroul doctorului acestuia. La acea oră, era de aşteptat ca doctorul să nu fie la birou şi a răspuns robotul; soţia lui Howard, presupunând că telefonul era ascultat, a pus la telefon mesajul pe care Howard îl înregistrase mai devreme. Acest lucru urma să ajute FBI-ul să confirme că Howard s-a întors acasă cu soţia lui. Aşa cum s-a dovedit, eforturile familiei Howard au fost inutile; în mod inexplicabil, agentul FBI care supraveghea casa nu a observat plecarea familiei Howard de acasă şi maşina lor nu a fost, de fapt, urmărită.
28. Un exemplu al interacţiunii dintre filaj şi contra-filaj este descris de Peter Wright, un fost funcţionar MI5 (serviciul de contra-informaţii britanic), în cartea sa *Spycatcher*. Wright spune că tehnicienii sovietici care operau la ambasada din Londra puteau să monitorizeze comunicaţiile echipelor mobile de filaj („Observatorii") folosite de MI5. Prin analizarea acestor comunicaţii şi corelarea lor cu propriile operaţiuni, sovieticii puteau deduce dacă o anumită

întâlnire dintre un ofițer de informații sovietic și sursa lui era posibil să fie supravegheată. Dacă era supravegheată, ofițerul era anunțat să anuleze întâlnirea. Serviciul britanic de contra-informații, conform celor scrise de Wright, a identificat această slăbiciune a sistemului de supraveghere când a detectat emisii electronice din ambasada rusă care au fost asociate direct cu operațiunile de interceptare radio ale comunicațiilor Observatorilor. Pe scurt, așa cum spune Wright, MI5 îi supraveghea pe sovieticii care îi supravegheau pe Observatori care, la rândul lor, îi supravegheau pe sovietici. Wright, *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer* (New York: Viking, 1987), 52-57, 91-93.

29. Pentru ilustrarea metodelor necesare realizării unei „căsuțe poștale impersonale", vezi descrierea făcută de John Barron rețelei de spionaj sovietice conduse de John Walker, *Breaking the Ring* (Boston: Houghton Mifflin, 1987), 80-96.

30. Declarațiile sub jurământ ale reprezentanților FBI în sprijinul mandatelor de arestare și percheziție în cazul Hanssen conțin citate ample din mesajele dintre Hanssen și KGB și dintre acesta și cu agenția rusă succesoare KGB, Sluzhba Vneshney Razvedki (Serviciul de Informații Externe sau SVR). În aceste mesaje, Hanssen refuza întâlniri față în față (chiar și în străinătate) din motive de securitate și insista să fie folosite aproape în exclusivitate căsuțe poștale impersonale. (Contactul inițial a fost stabilit prin poștă la reședința unui ofițer de informații sovietic; în câteva ocazii, s-a comunicat și prin telefon.) Declarațiile sub jurământ sunt disponibile la www.fas.org/irp/ops/ci/hanssen_affidavit.html, un manual veritabil referitor la căsuțele poștale impersonale.

31. Herbert Rommerstein și Stanislav Levchenco, *The KGB against the "Main Enemy": How the Soviet Intelligence Service Operates against the United States* (Lexington, Mass.: Lexington, 1989), 293. Neinformându-i pe ofițerii sovietici aflați la post în Viena, KGB-ul reducea astfel și riscul ca supravegherea de către SUA a acestora să compromită operațiunea Walker.

32. Nicholas Eftimiades, *Chinese Intelligence Operations* (Arlington, Va.: Newcomb, 1998), 33, 36-37.

33. La sfârșitul anului 1953, serviciul de informații sovietic, numit pe atunci MGB (Ministerul de Securitate a Statului), făcea parte din Ministerul de Interne (MVD); consolidarea acestor două autorități importante a fost rezultatul unei acțiuni în forță a fostului șef al serviciului de informații și conspirator important la Kremlin, Lavrenti Beria, în urma morții lui Stalin, în martie 1953. După arestarea și executarea lui Beria, în decembrie 1953, serviciul de informații sovietic a fost din nou separat de Ministerul de Interne și numit KGB (Comitetul de Securitate a Statului). Defectările au avut loc în aceste momente de schimbare în serviciul de informații. Cei cinci defectori (și țările în care au defectat) au fost: Yuri Rastvorov (Japonia); Pyotr Deryabin (Austria); Vladimir și Evdokia Petrova (Australia) și Nikolai Khokhlov (Germania de Vest). Vezi Gordon Brook-Shepherd, *The Storm Birds: Soviet Post-War Defectors* (Londra: Weidenfield și Nicholson, 1998), 57-131.

34. Conform lucrării Institutului Internațional de Cercetări de Pace din Stockholm, „Fact Sheet: Iraq: The UNSCOM Experience" (octombrie 1998), disponibil pe editors.sipri.se/pubs/Factsheet/UNSCOM.pdf, importanța celei mai mari locații de cercetare, dezvoltare și producție de arme biologice din Irak, al-Hakam, nu a

fost recunoscută până la defectarea lui Hussein al-Kamal, deşi inspectorii UNSCOM vizitaseră deja locaţia. În mod asemănător, defectarea în 1994 a unui om de ştiinţă important implicat în programul nuclear din Irak a oferit primele informaţii detaliate despre istoria programului şi mecanismele interne de funcţionare a acestuia. Judith Miller şi James Risen, "Defector Describes Iraq's Atom Bomb Push", *New York Times*, 15 august, 1998, A1.

35. Relatarea îi aparţine lui David C. Martin, *Wilderness of Mirrors* (New York, Harper and Row, 1980). Scrieri mai recente despre aceste dezbateri din cadrul comunităţii de informaţii americane se găsesc în *Cold Warrior: James Jesus Angleton, the CIA's Master Spy Hunter* de Tom Mangold (New York: Simon and Schuster, 1991) şi *Deception: The Invisible War between the KGB and the CIA* de Edward J. Epstein (New York: Simon and Schuster, 1989). Cărţile lui Mangold şi Epstein redau puncte de vedere clare, dar opuse, reflectând dificultatea de a trage o concluzie privind buna credinţă a unor defectori.

36. Chiar şi anterior, baloanele au fost folosite ca posturi de observaţie aeriene de către prima Republică Franceză, în 1794, şi de către Armata Unionistă în Războiul Civil American. În niciunul din cazuri nu s-a dobândit niciun succes notabil şi ambele armate şi-au abandonat mai târziu „forţele aeriene" în formare. Vezi William E. Burrows, *Deep Black: Space Espionage and National Security* (New York: Random House, 1987; New York: Berkley, 1988), 26-28.

37. Andrew, *Her Majesty's Secret Service*, 133.

38. William Mitchell, *Memoirs of World War I: „From Start to Finish of Our Greatest War"* (New York: Random House, 1960), 59, aşa cum e citat în cartea lui Russel F.Weigley, *The American Way of War* (Bloomington: Indiana University Press, 1977), 224.

39. O relatare profesionistă privind spionajul ştiinţific britanic în timpul celui de-al II-lea Război Mondial, scrisă de unul din experţii acestuia, o găsim în cartea *Most Secret War* de R.V Jones (Londra: Hamish Hamilton, 1978), republicată în Statele Unite sub titlul *The Wizard War: British Scientific Intelligence*, 1939-1945 (New York: Coward, McCAnn and Geoghegan, 1978).

40. John Prados, *The Soviet Estimate: U.S. Intelligence Analysis and Russian Military Strength* (New York: Dial, 1982), 38-50.

41. Prados, *The Soviet Estimate*, 29-30. Pentru o descriere mai detaliată vezi Curtis Peebles, *The Moby Dick Project: Reconnaissance Balloons over Russia* (Washington DC: Smithsonian, 1991).

42. Stephen E. Ambrose, *Eisenhower: The President*, vol. 2 din *Eisenhower* (New York: Simon and Schuster, 1984), 264-65.

43. Încă din 1946, Corporaţia RAND, un grup de experţi aflat sub contract cu Forţele Aeriene ale Armatei de la vremea respectivă, a fost solicitată să cerceteze fezabilitatea şi utilitatea sateliţilor pe orbita Pământului. În studiul său, RAND a arătat că sateliţii pot, printre alte lucruri, să servească drept „aeronavă de supraveghere care nu poate fi doborâtă de un duşman care nu deţine tehnici asemănătoare." Pentru un rezumat al studiilor RAND, vezi Walter A. McDougall, *The Heavens and the Earth: A Political History of the Space Age* (New York: Basic Books, 1985), 102-11. Pentru o descriere mai detaliată, vezi Merton E. Davies şi William R. Harris, *RAND's Role in the*

Evolution of Balloon and Satellite Observation Systems and Related U.S. Space Technology, R-3692-RC (Santa Monica, Calif.: RAND, septembrie 1988).

44. Ambrose, *Eisenhower*, vol.2, 228.

45. Referitor la decizia SUA de a construi un satelit de recunoaştere, eşecurile de început şi succesele programului, vezi McDougall, *The Heavens and the Earth*, 97-131, 190 şi 224 şi Dwayne A. Day, John M. Logsdon şi Brian Latell, *Eye in the Sky: The Story of the Corona Spy Satellites* (Washington DC: Smithsonian, 1998).

46. Vezi declaraţia Gen. Mr. B.L. Schriever, *Inquiry into Satellite and Missile Programs*, Audierile anterioare în faţa Subcomitetului de investigare privind starea de pregătire al Comisiei pentru serviciile armate din Senatul SUA, al 85-lea Congres, a doua sesiune, ianuarie 6-22, 1958, partea a doua, 1633-35.

47. Deşi se poate presupune că sovieticii au înţeles că existau astfel de capacităţi de recunoaştere, nu s-a considerat oportună atragerea atenţiei publice asupra acestui fapt. La vremea respectivă, Uniunea Sovietică, neclintită în decizia de a respinge planul "Open Skies", a considerat că recunoaşterea din spaţiu reprezintă o activitate de spionaj şi contravine dreptului internaţional în aceeaşi măsură ca recunoaşterea aeriană. Din cauza acestei poziţii, guvernul SUA era îngrijorat că o discuţie deschisă privind recunoaşterea din spaţiu va încuraja Moscova să o considere o problemă importantă. Aşadar, în ciuda discuţiilor publice despre recunoaşterea din spaţiu, la sfârşitul administraţiei Einsenhower, administraţia Kennedy, care nu vedea niciun motiv să-l stârnească pe Hruşciov, susţinând deschis dreptul Statelor Unite de a derula o astfel de recunoaştere, a luat „măsuri... pentru a trece programul de recunoaştere spaţială din zona gri în zona neagră." (Burrows, *Deep Black*, 107). Totuşi, aşa cum observă Walter McDougall, „până în 1963 bucuria [guvernului SUA] a luat sfârşit... Sovieticii au început să lanseze proprii sateliţi de spionaj... [care, în cele din urmă] au legitimat supravegherea din spaţiu." *The Heavens and the Earth*, 348.

48. Eric Schmitt, "*Spy-Satellite Unit Faces a New Life in Daylight*", New York Times, 3 noiembrie, 1992, A10.

49. În mod paradoxal, efectele de distorsiune generate de atmosfera terestră pot fi mai puţin problematice pentru fotografierea din spaţiu decât pentru cea aeriană. La începuturile fotografiei din spaţiu, faimosul expert în rachete Werner von Braun observa că „atunci când fotografiezi... din spaţiu, interferenţele şi turbulenţele sunt departe. Atmosfera este mult mai transparentă de deasupra decât de dedesubt." Pentru a ilustra afirmaţia, a sugerat următoarea demonstraţie: „Luaţi o coală de hârtie cerată. Ţineţi-o aproape de faţă şi veţi vedea ceva vag. Ţineţi-o pe o coală de ziar şi este perfect transparentă. O situaţie asemănătoare este şi aici." Discursul la a doua întâlnire anuală a Asociaţiei Armatei SUA, 26 octombrie 1956, citat în *The Heaven and the Earth* de McDougall, 224.

50. Această explicaţie a unui circuit cu cuplaj de sarcină este extrasă din Harold Hough, *Satellite Surveillance* (Port Townsend, Washington: Loompanics, 1991), 46-48.

51. Pentru că foloseşte lungimi de undă mari (comparativ cu lungimea de undă a luminii), radarul produce o imagine neclară, un simplu punct luminos pe ecran.

Modalitatea de a compensa pentru lungimile de undă mai mari este de a mări dimensiunea antenei. Din acest motiv, a fost perfectată o tehnică cunoscută drept radar cu apertură artificială (SAR), în care o antenă mică ce se mişcă în linie dreaptă are efectul unei antene mult mai mari. Cu procesoare puternice la bord, sistemele SAR colectează şi pun coroborează mii de „imagini" cu rezoluţie scăzută pentru a forma o imagine mult mai coerentă. Pentru mai multe detalii privind funcţionarea sistemelor SAR, vezi Charles Elachi, "Radar Images of the Earth from Space", *Scientific American*, (decembrie 1982), 54-61.

52. Departamentul de Apărare al SUA, *Conduct of the Persian Gulf War: Final Report to Congress* (Washington DC: U.S. Government Printing Office, 1992), 138, discută tactica „tank plinking" care a fost dezvoltată în timpul Războiului din Golf pentru a exploata acest fenomen. Un satelit poate utiliza şi un scanner multi-spectral care ia imagini ale ţintei folosind frecvenţe multiple din interiorul şi din exteriorul spectrului de lumină vizibilă. O imagine multi-spectrală poate furniza informaţii despre ţintă care nu pot fi detectabile cu ochiul liber. În timpul Războiului din Golf, de exemplu, imagistica multi-spectrală a fost folosită pentru a identifica zone de mică adâncime în apropierea zonelor de coastă, informaţii necesare pentru planificarea operaţiunilor cu amfibii. În plus, deoarece majoritatea imagisticii este acum formatată digital, datele pot fi manipulate mai uşor pentru a sublinia diferenţele mici, având ca rezultat un contrast mai mare şi, în consecinţă, o rezoluţie mai mare. Astfel, de exemplu, diferenţe topografice minore care nu pot fi detectate printr-o fotografie tradiţională pot fi redate mai clar prin tehnicile de procesare avansate.

53. Conform Ghidului privind spaţiul cosmic al Federaţiei oamenilor de ştiinţă americani (www.fas.org/spp/guide/index.html), China derulează operaţiuni de foto-recunoaştere spaţială încă din 1975, iar Franţa din 1995. Planurile japoneze subliniază necesitatea lansării a patru sateliţi (doi optici şi doi cu radar cu apertură artificială), începând cu 2002.

54. Vernon Loeb, "U.S. Is Relaxing Rules on Sale of Satellite Photos", *Washington Post*, 16 decembrie 2000, A3.

55. Lista este preluată dintr-un studiu de caz pregătit pentru Şcoala Guvernamentală John F. Kennedy la Universitatea Harvard. Rachel E. Billingslea, Matthew R. Domsalla şi Brian C. Payne, *The National Reconnaissance Office: A Strategy for Addressing the Commercialization of Space Imagery*, 6 aprilie 1999, disponibil la www.fas.org/eye/ADA366610.htm.

    Răspândirea imagisticii comerciale prezintă şi beneficii şi probleme. Pe de-o parte, guvernul îşi poate satisface o parte a necesităţilor în materie de imagistică prin achiziţionarea de produse de la comercianţi, aceasta permiţând serviciilor de informaţii să se concentreze asupra necesităţilor speciale care nu pot fi acoperite de sectorul comercial. Pe de altă parte, proliferarea sateliţilor comerciali pentru foto-recunoaştere face dificilă sarcina unui guvern de a ascunde amplasări strategice de forţe şi operaţiuni. (Statele Unite au încercat să rezolve problema prin rezervarea dreptului de stopare a activităţii sateliţilor, cu referire la sistemele pe care le licenţiază, pentru a împiedica operatorii să fotografieze anumite zone în perioade de criză, acest drept neextinzându-se însă şi asupra sistemelor operate de entităţi din afara SUA.) Pentru o scurtă descriere a acestui subiect, vezi Raportul Comisiei Naţionale de Evaluare a

Biroului Național de Recunoaștere din noiembrie 2000, la www.fas.org/irp/nro/commission.

56. Detectarea și analiza radiațiilor electro-magnetice emanate din surse radioactive sau detonări nucleare nu este considerată o componentă a ELINT. Vezi, de exemplu, definiția „informațiilor secrete electronice" în *Dictionary of Military and Associated Terms* al Departamentului de Apărare, Statul Major Reunit al SUA, JCS Publication 1-02 (Washington DC: Joint Staff, 12 aprilie 2001), 144, disponibil la www.dtic.mil/doctrine/jel/newspubs/jp1-02.pdf.

57. Așadar, undele electromagnetice generate de mașinile de scris electrice sau computere pot fi interceptate și analizate; în acest fel, textele sau datele introduse pe aceste dispozitive pot fi recuperate. O modalitate de a evita acest pericol este să cereți ca dispozitivele de acest tip să fie ecranate pentru a reduce acest fel de emanații și pentru a se împiedica încercările de interceptare.

    Un fenomen înrudit este emisia involuntară de semnale electromagnetice printr-un cablu. În unele cazuri, s-a descoperit că dispozitivele destinate codificării mesajelor emit semnale slabe care conțin text necodificat. Conform declarațiilor unui ofițer de contra-informații britanic, comunicațiile Ambasadei Franceze în Londra au fost vulnerabile deoarece francezii nu și-au ecranat corect dispozitivele de procesare a informațiilor, pentru a preveni astfel de emisii electronice involuntare. Ca rezultat, împreună cu textul codificat corect, cablul telex care ieșea din ambasadă transmitea și „ecoul" electronic slab, dar distinct al mesajelor diplomatice, așa cum fuseseră tastate inițial pe mașină. Dispozitivele de interceptare secrete instalate la mică distanță de ambasada franceză le-au permis britanicilor să citească mesajele diplomatice necodificate ale aliaților lor. Peter Wright, *Spycatcher*, 109-11.

58. Practica interceptării mesajelor antedatează folosirea radioului ca mijloc de comunicare; curierii erau capturați și scrisorile deschise înainte ca radioul să fi existat. În plus, comunicațiile prin telegraf puteau fi interceptate. În timpul Primului Război Mondial, britanicii au avut un avantaj în domeniul informațiilor deoarece companiile lor dețineau și operau multe din liniile internaționale de comunicații importante.

59. Tocmai pentru că mesajele radio pot fi ușor interceptate, mesajele importante sunt cel mai probabil trimise în formă criptată. Astfel, COMINT și criptanaliza, descifrarea codurilor și cifrurilor, sunt strâns legate, deși criptanaliza ar trebui privită probabil ca metodă de analiză a informațiilor (mai degrabă decât metodă de culegere de informații) și din acest motiv este discutată în următorul capitol.

60. Datorită preocupărilor continue privind confidențialitatea, este puțin probabil să se scrie în viitorul apropiat, o lucrare exhaustivă despre utilitatea COMINT în timpul Războiului Rece. Cu toate acestea, istoricii de la Agenția Națională de Securitate (NSA, serviciul SIGINT al SUA) susțin că succesul americanilor în descifrarea sistemelor sovietice de cifrare în anii ce au urmat celui de-al II-lea Război Mondial „s-a comparat cu succesele înregistrate în timpul celui de-al II-lea Război Mondial" și că pierderea acestei capacități în 1948 este „probabil cea mai semnificativă pierdere a serviciilor de informații din istoria SUA". Pierderea a fost în cele din urmă atribuită spionului William Weisband, un lingvist rus de a Agenția de Securitate a Forțelor Armate (predecesorul NSA). David A. Hatch și

Robert Louis Benson, *The Korean War: The Sigint Background* (2000), disponibil la: www.nsa.gov/korea/papers/sigint_background_korean_war.htm.

Dar fără accesul la arhivele secrete sovietice nu este posibil să se determine precis răul făcut de spionul american John Walker care a furnizat materiale criptografice maritime Uniunii Sovietice între 1968 şi 1985. În cel mai rău caz, se poate spune că materialele pe care Walker şi ceilalţi agenţi le-au furnizat KGB au oferit Uniunii Sovietice un „avantaj comparabil cu cel al Aliaţilor asupra naziştilor prin cunoaşterea Ultra. [Pe scurt, în cazul în care războiul ar fi izbucnit între cele două super-puteri,] Walker ar fi putut fi factorul decisiv pentru o victorie sovietică sau americană." Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (New York: Free Press, 1992), 176-78.

61. Pentru o discuţie completă despre comunicaţiile secrete ale marinei britanice în timpul Primului Război Mondial, vezi Patrick Beesley, *Room 40: British Naval Intelligence 1914-18* (New York: Harcourt Brace Jovanovich, 1982).

62. Literatura referitoare la criptografia americană şi britanică în timpul celui de-al II-lea Război Mondial este enormă. Pentru o scurtă trecere în revistă vezi G.J.A. O'Toole, *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action from the American Revolution to the CIA* (New York: Atlantic Monthly, 1991), 384-97.

63. În mesajele lor, japonezii s-au referit la ţinta pe care o vizau ca *AF*. Ofiţerii de informaţii din Hawaii au crezut că *AF* era codul pentru Midway, dar cei din Washington au crezut că poate fi vorba de altă locaţie, cum ar fi Johnston Island, Oahu sau chiar coasta de vest a Statelor Unite. Pentru a avea confirmarea că japonezii intenţionau să atace Midway, serviciile de comunicaţii ale Marinei Hawaii l-au pus pe comandantul S.U.A. din Midway să trimită un mesaj către Hawaii conform căruia insula rămânea fără rezerve de apă. Aşa cum se anticipa, japonezii au interceptat mesajul şi două zile mai târziu o comunicaţie radio japoneză (interceptată de Statele Unite) raporta către Tokyo că rezervele de apă din *AF* erau scăzute, aceasta confirmând indirect că *AF* era într-adevăr Midway. Edwin T. Layton, Roger Pineau şi John Costello, "*And I Was There": Pearl Harbour and Midway – Breaking the Secrets* (New York: Morrow, 1985), 421-22.

64. Pentru o descriere a bătăliei şi a succesului serviciilor secrete din spatele acesteia, vezi Layton, *„And I Was There"*.

65. Vezi Comisia Specială pentru Activitatea Serviciilor de Informaţii a Senatului SUA, *Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs*, S.Rpt. 99-522 (Washington DC: Government Printing Office, 1986), 33-34, 80-81. În plus, Uniunea Sovietică a întreţinut mulţi ani (aşa cum Rusia a făcut-o până în 2002) un dispozitiv puternic de interceptare la Lourdes, Cuba. Având un personal de 1500 de angajaţi ruşi, dispozitivul monitoriza traficul de voce şi date din SUA. O descriere a acestui dispozitiv se găseşte în secţiunea „Concluzii" a unui proiect de lege al Camerei Reprezentanţilor a SUA din 19 iulie 2000, „Russian-American Trust and Cooperation Act of 2000", HR 4118, Congresul 106, sesiunea 2.

66. Peter Wright, fostul agent MI5, scrie în memoriile sale că „analiza traficului" era folosită de serviciile secrete sovietice pentru a reduce eficienţa eforturilor britanice de monitorizare a operaţiunilor secrete sovietice din Londra şi din

împrejurimile acesteia. Aşa cum am menţionat anterior, sovieticii monitorizau comunicaţiile echipelor de supraveghere britanice din ambasada lor de la Londra. Faptul că aceste comunicaţii erau cifrate era nesemnificativ; dimpotrivă, le făcea „să iasă în evidenţă" în traficul radio necifrat din oraş. Prin analizarea acestor semnale radio, în special volumul activităţii radio, sovieticii puteau să deducă momentele în care operaţiunile de supraveghere ale contra-informaţiilor britanice (MI5) erau în derulare şi dacă una din operaţiunile lor era în pericol să fie compromisă din această cauză. După părerea lui Wright „ruşii culegeau majoritatea informaţiilor chiar din trafic, mai degrabă decât din conţinutul mesajelor." *Spycatcher*, 52-53.

67. Vezi David Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943* (Boston: Houghton Mifflin, 1991), 144-45, 215-16 şi 244-51 şi Patrick Beesly, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre, 1939-45* (Garden City, N.Y.: Doubleday, 1978), 55-56, 97-98, 116 şi 195.

68. Pentru o descriere a acestei operaţiuni, vezi David E. Murphy, Sergei A. Kondrashev şi George Bailey, *Battleground Berlin: CIA vs. KGB in the Cold War* (New Heaven, Conn.: Yale University Press, 1997), cap.11. Existenţa tunelului a fost trădată sovieticilor de către George Blake, un spion sovietic în Serviciul Secret de Informaţii Britanic (SIS); cartea redă un raport al unei şedinţe de planificare SIS/CIA pe care Blake l-a furnizat sovieticilor (449-53) şi dezbate dacă sovieticii au folosit faptul că ştiau dinainte despre monitorizare pentru a induce în eroare Statele Unite şi Marea Britanie (423-28).

69. Această operaţiune cu numele de cod "Ivy Bells" este descrisă în detaliu în cartea lui Sherry Sontag şi Cristopher Drew: *Blind Man's Bluff: The Untold Story of American Submarine Espionage* (New York: Public Affairs, 1998), 158-83 şi passim.

70. Wright, *Spycatcher*, 81-86. Mai recent, serviciile secrete sovietice au putut, din cauza practicilor deficiente în materie de securitate ale SUA, să aibă acces la maşinile de scris electrice trimise Ambasadei Americane din Moscova. (Departamentul de Stat al SUA a trimis maşini de scris în Uniunea Sovietică cu un transport comercial neînsoţit.) Prin inserarea unor dispozitive de interceptare sofisticate în maşinile de scris, sovieticii au putut să „citească" materialele (clasificate sau nu) care erau scrise. Vezi Comisia Specială pentru Activitatea Serviciilor de Informaţii a Senatului SUA, *Meeting the Espionage Challenge*, 34-35; pentru o relatare neoficială a acestui episod vezi Kessler, *Moscow Station*, 92-97.

71. Pentru o discuţie privind dificultăţile de interceptare secretă a comunicaţiilor prin fibră optică, în special a celor ce trec pe sub ocean, vezi Neil King Jr., "As Technology Evolves, Spy Agency Struggles to Preserve Its Hearing", *Wall Street Journal*, 23 mai 2001, A1.

72. De exemplu, în 2000 Comisia Specială pentru Activitatea Serviciilor de Informaţii a Senatului SUA a raportat după cum urmează: „Comitetul este din ce în ce mai îngrijorat de incapacitatea accentuată a Agenţiei de Securitate Naţională (NSA) de a se ridica la nivelul provocărilor tehnologice şi de a furniza liderilor americani informaţii SIGINT vitale." *Report of the Senate Select Committee on Intelligence Authorizing Appropriations for Fiscal Year 2001 for the Intelligence Activities of the United States Government and the*

Central Intelligence Agency Retirement and Disability System and for Other Purposes, S.Rep. 106-279, 4 mai 2000.

73. Jeffrey Richelson, *Sword and Shield: The Soviet Intelligence and Security Apparatus* (Cambridge, Mass.: Ballinger, 1986), 103-105. vezi şi Curtis Peebles, *Guardians: Strategic Reconnaisance Satellites* (Novato, Calif.: Presidio, 1987), 279-89. La fel ca sateliții de foto-recunoaştere, sateliții ELINT au sarcini specifice de culegere de informații care determină orbita şi numărul de sateliți necesari. În general, localizarea ELINT şi urmărirea sistemelor militare ale altei țări necesită numeroşi sateliți de altitudine joasă. Este probabil să se amplaseze pe o orbită elipsoidală un satelit pentru culegerea de informații ELINT pentru a determina caracteristicile electronice exacte ale unui sistem militar. Pe o astfel de orbită satelitul, pe măsură ce se apropie de punctul cel mai îndepărtat de Pământ, pare să zboare relativ încet deasupra zonei țintă. Astfel, are mai mult timp să capteze şi să înregistreze semnalele dorite. Desigur, este posibil ca un satelit să se plaseze pe o orbită geo-sincronică. (Un satelit aflat pe o orbită geo-sincronică înconjoară Pământul deasupra Ecuatorului, realizând un cerc complet pe zi, astfel, de pe pământ pare să „atârne" inert deasupra unui anumit punct de pe Ecuator.) Aceasta permite receptorilor ELINT ai satelitului să stea „fixați" continuu deasupra unei țări, dezavantajul fiind distanța mare de transmițători. Aşadar, utilitatea unui sistem geo-sincronic depinde de intensitatea semnalului receptat şi de sensibilitatea receptorilor de la bordul satelitului.

74. Calculul se face după cum urmează: unda radio emisă de un radar călătoreşte cu viteza luminii sau trei sute de mii de kilometri pe secundă. Aşadar, poate călători cu 300.000/500=600 km între impulsuri. Deci, dacă unda trebuie să atingă ținta şi să se întoarcă la radar înainte ca următorul impuls să fie emis, ținta nu poate fi la mai mult de trei sute de kilometri de radar. Jones, *The Wizard War*, 198.

75. Relatarea acestui episod este extrasă din *The Electronic Spies* (Alexandria, Va.: Time-Life, 1991), 106-107.

76. Conform definiției oficiale a SUA, senzorii MASINT „includ, dar nu sunt limitați la, sisteme radar, laser, infraroşii, acustice, nucleare, de detectare a radiațiilor, spectro-radiometrice şi seismice, precum şi sisteme de recoltare de materiale lichide, solide şi gazoase" ale căror date „când sunt colectate, procesate şi analizate generează informații care detectează, recoltează, identifică sau descriu semnăturile (caracteristicile distincte) ale surselor țintă fixe şi dinamice". MASINT a fost clasificat formal ca un domeniu al culegerii de informații în 1986, iar în 1993 DCI şi secretarul apărării au creat Biroul Central MASINT (CMO) în cadrul Agenției de Informații a Apărării pentru a supraveghea şi monitoriza activitățile de apărare MASINT. Vezi secțiunea 7, "MASINT: Measurement and Signals Intelligence", a Camerei Reprezentanților a SUA, Comisia Specială Permanentă pentru Activitatea Serviciilor de Informații, *IC21: Intelligence Community in the 21st Century* (Washington DC: U.S. Government Printing Office, 1996), disponibil la www.fas.org/irp/congress/1996_rpt/ic21/index.html.

77. Pentru o descriere generală a tehnologiei utilizate în monitorizarea seismică în cazul testelor nucleare subterane, vezi Biroul de Evaluare a Tehnologiilor din cadrul Congresului SUA, *Seismic Verification of Nuclear Testing Treaties*, OTAISC-361 (Washington DC: Government Printing Office, mai 1988).

Pentru detectarea de la distanță a testelor nucleare la suprafață. Vezi Peebles, *Guardians*, 331-42.

78. Pentru o descriere literară a culegerii de informații prin folosirea sonarului, vezi Tom Clancy, *The Hunt for Red October* (Annapolis, Md.: Naval Institute, 1984). Descrieri ştiinţifice sunt ceva mai greu de găsit în surse deschise. Totuşi, vezi Joel S. Witt, „Advances in Antisubmarine Warfare", *Scientific American*, februarie 1981. Referitor la posibilitatea de detectare a submarinelor prin alte modalități, vezi Tom Stefanick, „The Nonacoustic Detection of Submarines", *Scientific American*, martie 1988.

79. Practic, nu există niciun acord universal în virtutea căruia legislația internațională să permită recunoaşterea din satelit. Tratatul privind Spațiul Cosmic din 1967, de exemplu, nu se referă direct la problema recunoaşterii din spațiul cosmic. Tratatele privind controlul armamentului fac referire la „mijloacele tehnice naționale de verificare" dar nu definesc aceşti termeni. De exemplu, articolul IX din Tratatul de neproliferare a armelor strategice din 1991 (între SUA şi fosta Uniune Sovietică) stipulează ca „mijloacele tehnice naționale de verificare [să fie folosite] ... în conformitate cu principiile general recunoscute ale legislației internaționale."

Poziția SUA a fost că suveranitatea unei națiuni nu se extinde şi asupra spațiului cosmic (adică, dincolo de atmosfera terestră) şi prin urmare, o națiune este liberă să deruleze activități de recunoaştere din spațiul cosmic, aşa cum este şi în largul mării. La începutul erei spațiale părerea Uniunii Sovietice era că recunoaşterea din spațiul cosmic era la fel de ilegală ca şi recunoaşterea aeriană care implica survolarea neautorizată a teritoriului altei națiuni. Totuşi, din motive obiective, folosirea efectivă a spațiului de către un număr de state, inclusiv fosta Uniune Sovietică, au făcut din problema ilegalității o temă de dezbatere pentru legislația internațională.

80. Toate țările păstrează secrete costurile reale ale sistemelor implicate în recunoaşterea din spațiul cosmic. Pentru o evaluare neclasificată vezi documentul Biroului pentru Buget al Congresului SUA, *U.S. Costs of Verification and Compliance under Pending Arms Treaties* (Washington DC: Government Printing Office, 1990), 43-47. Deoarece costurile de construire şi lansare a sateliților sunt mari, tendința a fost să se achiziționeze câțiva sateliți performanți şi aceştia să fie configurați astfel încât să poată sta mult timp în spațiu (poate şapte sau mai mulți ani). Această abordare, deşi economicoasă într-un fel, are dezavantajul că poate lăsa o țară în „întuneric" în cazul în care se întâmplă ceva neaşteptat cu unul dintre sateliții săi sau dacă se întâmplă ceva într-o zonă din lume care nu poate fi acoperită uşor de orbitele sistemelor de recunoaştere existente.

O strategie mai flexibilă şi de perspectivă ar fi construirea mai multor sateliți mai ieftini cu durată de viață mai scurtă. În 1996, un studiu colectiv al Comisiei Speciale Permanente pentru Activitatea Serviciilor de Informații a Camerei Reprezentanților din SUA menționa că „transformările continue ale capacităților de procesare... permit amplasarea de sateliți care nu numai că sunt mai uşori şi mai ieftini, dar sunt şi mai inteligenți... Pentru unele aplicații, la un moment dat „micro-sateliții" amplasați în „nori"... ar putea implica culegerea distribuită şi diviziunea sarcinilor, astfel permițând reconstituirea ieftină sau înlocuirea anumitor părți." *IC21: Intelligence Community in the 21st Century*

(Washington DC:. Government Printing Office, 1996), 108, disponibil la www.fas.org/irp/congress/1996_rpt /ic21/index.html.

Totuşi, în general sateliţii mai ieftini sunt mai puţin eficienţi şi, oricum, lansarea implică cele mai multe costuri. Alegerea strategiei va fi determinată de priorităţile de culegere a datelor stabilite de guvern şi de rafinamentul tehnologiei deţinute de cei care construiesc sateliţii. Pentru o scurtă analiză a acestora şi a problemelor aferente, vezi Codevilla, *Informing Statecraft*, 313-24.

81. Vezi Victor Suvorov, *Inside the Soviet Army* (New York: Macmillan, 1982), 106. Schimbări minore dar imprevizibile ale orbitei pot fi realizate prin lovirea satelitului cu rachete de mici dimensiuni, numărul şi magnitudinea acestor manevre fiind limitată de capacitatea rezervorului de combustibil al satelitului.

82. Departamentul de Apărare al SUA, *Conduct of the Persian Gulf War*, 338, 710.

83. Citatele sunt dintr-o declaraţie comună a secretarului pe probleme de apărare al SUA, William Cohen, şi a Gen. Henry H. Shelton, preşedintele Statului Major Reunit, în faţa Comisiei pentru Serviciile Militare a Senatului SUA, 14 octombrie 1999, disponibil la www.fas.org/man/dod-01/ops/docs99/b10141999_bt478-99.htm.

84. Pentru diferite variante de activităţi care se pot derula sub acoperirea unui camion obişnuit sau a unei dube, vezi Desmond Ball, "Soviet Signals Intelligence: Vehicular Systems and Operations", *Intelligence and National Security* 4, nr.1 (ianuarie 1989), 5-27. Pentru variante mai neconvenţionale, vezi Alfred Price, *The History of U.S. Electronic Warfare: The Renaissance Years* (Alexandria, Va.: Association of Old Crows, 1989), 89, 160-61, pentru o descriere a proiectului U.S. Moonbounce, care intercepta semnalele radar sovietice reflectate de pe lună.

85. În plus, miniaturizarea permite Departamentului de Apărare al SUA să dezvolte dispozitive de recunoaştere de mărimea unei palme şi roboţi de cercetare în miniatură, pentru a fi folosiţi pe câmpul de luptă. Avioanele spion de mici dimensiuni (numite „micro-aero-vehicule" sau MAV) şi roboţii oferă unităţilor de luptă mici capacitatea de a cerceta mediul înconjurător. Michael A. Dornhein, "Tiny Drones May Be Soldier's New Tool", *Aviation Week and Space Technology*, 8 iunie 1998, 42-48 şi Kevin Kaley, "Robot Scouts May Gather Info for U.S. Marine Corps", *Defense News*, 24 iulie 2000, 20.

86. Stansfield Turner, *Secrecy and Democracy: The CIA in Transition* (Boston: Houghton Mifflin, 1985; New York: Harper and Row, 1986), 92. După Războiul Rece, Turner a susţinut că „Washington-ul poate construi cu uşurinţă un sistem care să detecteze orice activitate semnificativă la suprafaţa pământului, zi sau noapte, indiferent de condiţiile meteorologice sau topografice şi cu o asemenea frecvenţă încât evitarea deliberată a acestuia ar fi dificilă... Preţul de achiziţionare de 5 miliarde USD şi costurile de întreţinere de 1 miliard pe an [,]... sunt un chilipir." În opinia fostului DCI, încă mai există loc pentru culegerea de informaţii din surse umane în era de după Războiul Rece, dar, în general, „noua ordine mondială va genera sisteme tehnice care vor servi drept sabie, mijloace de ultimă oră în culegerea de informaţii, iar operaţiunile de spionaj bazate pe surse umane vor fi floreta, fiecare fiind folosite judicios în funcţie de necesităţi." Turner, „Inteligence for a New World Order", *Foreign Affairs* 70, nr.4 (toamna anului 1991): 151, 159.

87. În cei zece ani în care a lucrat pentru serviciile de informaţii americane, Col. Ryszard J. Kuklinski, ofiţer în armata poloneză, a furnizat, printre altele, şi sute

de pagini de documente secrete, inclusiv planurile de luptă sovietice pentru un război în Europa. Pentru relatări privind cariera de spion a colonelului Kuklinski, vezi Benjamin Weiser, "Polish Officer Was U.S.'s Window on Soviet War Plans", *Washington Post*, 27 septembrie 1992, A1 şi "A Question of Loyalty", *Washington Post Magazine*, 13 decembrie 1992, 9-30.

88. Jozef Garlinski, *The Enigma War* (New York: Scribner, 1979), 16. Agentul german Hans-Thilo Schmidt a fost descris de istoricul David Kahn drept „spionul care a avut cea mai mare influenţă asupra sorţii celui de-al II-lea Război Mondial". *Kahn on Codes: Secrets of the New Cryptology* (New York: Macmillan, 1983), 76-88.

89. HUMINT poate juca şi aici un rol. De exemplu, conform unor relatări, colonelul Kuklinski a furnizat informaţii despre care dintre „ţintele sovietice vizibile prin satelit erau false şi care erau adevărate". În plus, rapoartele lui Kuklinski au ajutat serviciile secrete americane să monitorizeze programul militar sovietic de construire a unei reţele de buncăre de comandă şi control ascunse pe care sovieticii şi aliaţii lor intenţionau să le folosească în cazul unui război în Europa. Weiser, "Polish Officer Was U.S.'s Window on Soviet War Plans".

90. Vezi R. Jeffrey Smith, "Iraq's Secret A-Arms Effort: Lessons for the World", *Washington Post*, 11 august 1991, C1; R. Jeffrey Smith, „Iraq's Nuclear Powers Underestimated by U.S.", *Washington Post*, 13 noiembrie 1991, A45; R. Jeffrey Smith şi Glenn Frankel, "Saddam's Nuclear Weapons Dream: A Lingering Nightmare", *Washington Post*, 13 noiembrie 1991, A1.

91. Smith, "Iraq's Secret A-Arms".

92. Pentru opinii privind rolul serviciilor secrete în „dezvoltarea sistemului militar", vezi James R. FitzSimonds, "Intelligence and the Revolution in Military Affairs", în *U.S. Intelligence at the Crossroads: Agendas for Reform*, ed. Roy Godson, Ernest R. May şi Gary Schmitt (Washington DC: Brassey's [U.S.], 1995), 265-87. Printre sarcinile care trebuie îndeplinite pentru a exploata la maximum TECHINT în scopuri tactice, FitzSimonds menţionează următoarele: „acoperire globală – arie extinsă, condiţii meteorologice diverse, identificare zi/noapte a ţintelor mobile şi fixe din zonele de coastă, în aer şi în spaţiu"; „monitorizarea continuă a ţintelor... în timp real (sau aproape în timp real)", inclusiv „evaluarea consecinţelor războiului" şi „transmiterea în timp real a informaţiilor privind localizarea ţintei către focosul rachetei, inclusiv către rachetele aflate în zbor" (268).

93. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton N.J.: Princeton University Press, 1949; retipărit în 1966), 3-4. Kent, un veteran al Biroului pentru servicii strategice (OSS), serviciul secret american în timpul celui de-al II-lea Război Mondial, a oferit o teorie specific americană privind culegerea de informaţii imediat după cel de-al II-lea Război Mondial.

94. V. Zaykin, " 'Secret' Classification Removed", *Izvestiya*, 3 septembrie 1988, 2, retipărit şi tradus în Federal Broadcast Information Service (FBIS), *Soviet Report*, 8 septembrie 1988, (FBIS-SOV-88-174), 53-54.

95. Campania strategică de bombardare a avut rezultate mixte. Spre meritul lor, economiştii OSS proiectaseră un sistem relativ sofisticat şi util de selectare a ţintelor. Dar au omis multe date de război privind economia germană care i-ar fi ajutat să-şi exploateze la maxim analiza strategică. Despre aceste chestiuni,

vezi Stephen Peter Rosen, "Winning the Next War: Innovation and the Modern Military (Ithaca, N.Y.: Cornell University Press, 1991), 148 – 70.

96. Luându-se în considerare depedența totală a proiectului de materialele din surse deschise şi de metodologiile care, fiind elaborate în mediul academic, sunt cunoscute în țara a cărei birocrație a fost studiată, ne putem întreba de ce această operațiune trebuie efectuată de un serviciu de informații. Evident, nu este necesar, dar eventuala sa plasare într-un centru de cercetare neclasificat depinde de o serie de factori. Pe de o parte, ar putea fi mai uşor să se recruteze personal pentru un astfel de centru deschis, iar activitatea sa ar fi mai uşor de împărtăşit comunității academice. Pe de altă parte, procedurile speciale greoaie ar fi necesare pentru a integra acest material provenit din surse deschise în informații secrete, sau pentru a le utiliza în activitățile derulate de serviciile secrete. De exemplu, dacă informațiile au fost necesare la recrutarea unui funcționar pentru spionaj, solicitarea ar trebui camuflată, pentru a se ascunde motivul.

97. Donald E. Queller, The Office of Ambassador in the Middle Ages (Princeton, N.J.: Princeton University Press, 1967), 90.

98. Lucrarea "Long Telegram", scrisă de George Kennan în 1946, când era însărcinatul cu afaceri la Moscova, reprezintă un exemplu clasic de raport diplomatic de acest tip. De-a lungul Războiului Rece, telegrama lui Kennan cu privire la Uniunea Sovietică a constituit temeiul intelectual a ceea ce a devenit strategia americană de menținere sub control a URSS. Pentru textul telegramei lui Kennan, vezi Kenneth M. Jensen, ed., Origins of the Cold War: The Novikov, Kennan, and Roberts "Long Telegrams" of 1946 (Washington D.C.: United States Institute of Peace, 1991).

99. În text este prezentată activitatea cotidiană a ataşatului militar, activitate care în esență nu este secretă, deşi acesta ar putea încerca să călătorească în sau pe lângă zone restricționate pentru a urmări obiective pe care țara gazdă ar prefera ca el să nu le urmărească. În plus, ca orice post diplomatic, cel de ataşat militar se poate utiliza ca acoperire pentru un ofițer de informații.

CAPITOLUL 3: CARE ESTE SEMNIFICAȚIA INFORMAȚIILOR? ANALIZA ŞI PRELUCRAREA

1. Acest aspect ridică întrebarea dacă se poate crea un cifru "imbatabil". Lăsând la o parte anumite considerații confuze privind natura caracterului aleatoriu, răspunsul este da, se poate crea un cifru imposibil de spart. Acest lucru implică utilizarea a ceea ce poartă denumirea de "cod de unică folosință". De exemplu, luați în considerare următorul sistem care implică un cod super-cifrat. Prima etapă constă în transformarea în cod a mesajului transmis. (Acest cod diferă de cel abordat de text prin faptul că grupurile codului sunt numere formate din patru cifre şi nu grupuri de patru litere). De exemplu, cu ajutorul unui manual de coduri, expresia "războiul începe mâine" ar putea fi codificată sub forma "4251 1712 2844." În următoarea etapă, la aceste grupuri de numere se adaugă o serie de numere generate aleatoriu (cum ar fi "3648 5217 8150…"), luate în ordinea în care se regăsesc într-un tabel de numere, "un cod" după care au copii doar expeditorul şi destinatarul. Prin adunare, obținem:

4251 1112 2844
3648 5217 8150
7899 6329 0994

(Dacă suma depăşeşte 9999, se renunţă la primul "1".) Apoi se transmite seria finală de grupuri de numere. La primire, procesul se inversează. După ce-şi consultă copia codului care conţine grupele de numere aleatorii, destinatarul scade cifrele adăugate din cele pe care le primise, obţinând primul set de numere, care apoi este decodat utilizând manualul de coduri. Sistemul se securizează în felul următor: după ce se utilizează o singură dată, hârtia cu o serie de numere aleatorii se distruge şi nu se mai utilizează niciodată. Dacă nu deţine "cheia" unui anumit mesaj, inamicul nu poate decripta mesajul, chiar dacă a obţinut manualul de coduri, întrucât cifrele adăugate nu au nicio legătură între ele. Prin urmare, numerele transmise nu vor prezenta un caracter sistematicpe baza căruia un criptanalist să poată să spargă cifrul.
Din păcate, "codul" (ale cărui copii trebuie furnizate în mod securizat atât expeditorului, cât şi destinatarului) trebuie să aibă cel puţin lungimea tuturor mesajelor care urmează să fie transmise. De aceea, sistemul nu este practic atunci când este dificil să se securizeze comunicaţiile dintre expeditor şi destinatar sau atunci când este vorba despre un trafic mare de mesaje. Vezi John Earl Haynes şi Harvey Klehr, Venona: Decoding Soviet espionage in America (New Haven, Conn.: Yale University Press, 1999), cap. 2, care prezintă modul în care cript-analiştii americani au exploatat utilizarea defectuoasă de către sovietici a sistemului codului de unică folosinţă pentru a citi mii de mesaje cu detalii referitoare la spionajul sovieticilor din Statele Unite.

2. Vezi David Kahn, The Codebreakers: The Story of Secret Writing (New York: Macmillan, 1967), pentru cea mai amplă analiză publică a istoriei criptografiei. Cu toate acestea, de la publicarea cărţii sale, prezentările succeselor obţinute de britanici în spargerea cifrurilor germane în timpul celui de-al doilea Război Mondial au reprezentat un capitol nou şi important pentru istoria criptografiei. Noutatea propusă de Kahn se află în Kahn on Codes: Secrets of the New Criptology (New York: Macmillan, 1983); vezi, printre alte eseuri, "The Spy Who Most Affected World War II" şi "Codebreaking in World War I and II: The Major Successes and Failures, Their Causes and Their Effects," 76 – 88 şi 99 – 119. În plus, vezi şi "Seizing the Enigma: The Race to Break the German U – Boat Codes, 1939 – 1943", de acelaşi autor (Boston: Houghton Mifflin, 1991).

3. Vezi Patrick Beesly, Room 40: British Naval Intelligence 1914 – 18 (New York: Harcourt Brace Jovanovich, 1982), 3 – 7, 22 – 33.

4. Vezi Barbara Tuchman, The Zimmermann Telegram (New York: Macmillan, 1958, 1966), pentru o prezentare completă a acestui incident.

5. Herbert O. Yardley, The American Black Chamber (Indianapolis: Bobbs – Merrill, 1931; re-editată, New York: Ballantine, 1981), 4.

6. Kahn, The Codebreakers, 348.

7. O astfel de teorie matematică a fost elaborată la începutul anilor 1930 de către criptografii matematicieni polonezi care au obţinut primele succese pentru Polonia şi apoi, reuşitele ulterioare împotriva sistemului german Enigma. Vezi,

de exemplu, Josef Garlinski, The Enigma War (New York: Scribner, 1979), 25, 196 – 204.

8. Pe lângă cărțile citate deja, această literatură include şi următoarele lucrări: Peter Calvocoressi, Top Secret Ultra (New York: Ballantine, 1980); Josef Garlinkski, The Enigma War: The Inside Story of the German Enigma Codes and How the Allies Broke Them (New York: Scribner, 1979); Ronald Lewin, Ultra Goes to War (London: Hutchinson, 1978; New York: McGraw – Hill, 1978); şi F. W. Winterbotham, The Ultra Secret (New York: Harper and Row, 1974).

9. De exemplu, acum există un ziar cu circuit academic, intitulat Cryptologia, care abordează aceste subiecte.

10. Criptanalistul poate fi ajutat de numeroase posibile greşeli de utilizare a unui cifru. De exemplu, procedura germană de la începutul Celui de-al Doilea Război Mondial, de repetare, la începutul fiecărui mesaj, a unei chei din trei litere, a fost extrem de dăunătoare: pe criptanaliştii britanici i-a ajutat foarte mult faptul că ştiau că prima şi a patra literă a un unui text erau identice (la fel şi a doua şi a cincea, a treia şi a şasea). Vezi Gordon Welchman, The Hut Six Story: Breaking the Enigma Codes (New York: McGraw – Hill, 1982), 59 – 73, pentru a vedea cum au exploatat britanicii această eroare a germanilor. La fel, formatele obişnuite ale mesajelor, saluturile standard sau alte expresii uzuale pot furniza indicii importante criptanaliştilor. Welchman menționează că el şi alți criptanaliști britanici "l-au simpatizat pe un ofițer german care a stat o perioadă mai lungă în Depresiunea Qattara din Africa de Nord şi raporta zilnic că nu are nimic de raportat. În astfel de cazuri, am fi vrut să le solicităm comandanților britanici să-l lase în pace" (132).

11. De exemplu, s-a raportat că rețeaua de spionaj Walker a furnizat serviciilor secrete sovietice o mare cantitate de material cifrat, acestea putând astfel să decripteze un milion de mesaje secrete americane. Pentru o prezentare succintă a cazului Walker, vezi Christopher Andrew şi Oleg Gordievsky, KGB: The Inside Story of its Foreign Operations from Lenin to Gorbachev (New York: Harper Collins, 1990), 524 – 31.

12. Kahn, The Codebreakers, 603; Ronald Lewin, The American Magic: Codes, Ciphers and the Defeat of Japan (New York: Farrar Straus Giroux, 1982), 113.

13. Kahn, The Codebreakers, 604.

14. Lewin, The American Magic, 116 – 17. Vezi şi Edwin T. Layton, "And I Was There": Pearl Harbor and Midway – Breaking the Secrets (New York, Morrow, 1985), 453 – 56, pentru o discuție despre acest incident.

15. Lewin, The American Magic, 117.

16. Dificultățile de elaborare a unui nou sistem criptografic şi de distribuire a acestuia către cei implicați ar putea explica cu uşurință de ce japonezii s-au limitat să anunțe data unei schimbări de cod deja planificate. Mai mult, autoritățile japoneze au transmis ambasadei lor din Lisabona, Portugalia fiind neutră, o solicitare de "ziare, în special pentru ziarul anti - guvernamental Chicago Tribune, cu cât mai multe numere anterioare." Deşi neconcludent, acest lucru sugerează că autoritățile japoneze ştiau despre articolul din Tribune referitor la Midway şi că le preocupa îndeajuns de mult posibila sa semnificație pentru a dori să-l citească. Prezentarea succintă a informațiilor secrete Magic

(derivate din traficul telegramelor diplomatice japoneze interceptate), din 11 septembrie 1942, citat în B. Nelson Macpherson, "The Compromise of U.S. Navy Cryptanalysts after the Battle of Midway," Intelligence and National Security 2, nr. 2, (aprilie 1987): 321. Prezentarea nu indică data mesajului transmis de la Tokyo la Lisabona.

17. Christopher Andrew, Her Majesty's Secret Service: The Making of the British Intelligence Community (New York: Viking, 1986), 331 – 32.

18. Bob Woodward şi Patrick E. Tyler, "Libyan Cables Intercepted and Decoded," Washington Post, 15 aprilie 1986, A1.

19. Stephen Engleberg, "US Aides Worried over Libya Cables,", New York Times, 17 aprilie 1986, A24.

20. Lewin, Ultra Goes to War, 99 – 103. Vezi şi F.H. Hinsley, et al., British Intelligence in the Second World War: Its Influence on Strategy and Operations (New York: Cambridge University Press, 1979) 1, anexa 9 ("Intelligence in advance of the GAF Raid on Coventry, 14 noiembrie 1940"), 528 – 48.

21. Pentru o face o analogie, vă puteți imagina că vă confruntați cu un set de grafice care nu au nici inscripții şi nici gradații pentru axele x şi y şi că vi s-a comunicat doar natura fenomenului ale cărui diferite aspecte sunt prezentate în grafice. Apoi, cuiva i se cere să explice semnificația fiecărui grafic şi să prezinte fenomenul în mod detaliat. Aşa cum menționează Angelo Codevilla, "Spre deosebire de inginerii care au proiectat-o, serviciul de informații care interceptează telemetria nu o cunoaşte, aşa că trebuie să propună scara în care urmează să se citească fiecare canal." (Angelo Codevilla, Informing Statecraft: Intelligence for a New Century, [New York: Free Press, 1992, 122). Verificarea finală a propunerilor avansate şi a procesului ca un tot unitar constă în producerea unui model de rachetă coerent ca structură şi care să corespundă cu orice date obținute din alte surse.

22. SALT II a interzis utilizarea criptării telemetrice dacă aceasta împiedica verificarea modului în care se respectau prevederile tratatului. Unii au argumentat că insistența SUA de a include în tratat această prevedere privind interzicerea criptării a avut efecte adverse întrucât Uniunea Sovietică a fost alertată cu privire la succesele obținute de americani în interceptarea şi exploatarea telemetriei rachetelor sovietice. Alții au susținut că succesele obținute de spionajul sovietic împotriva sateliților americani de culegere SIGINT "ar fi putut contribui la hotărârea sovieticilor de a cripta telemetria". (Senatorul Gordon J. Humphrey, "Analysis and Compliance Enforcement," în Verification and SALT: The Challenge of Strategic Deception, ed. William C. Potter, [Boulder, Colo.: Westview, 1980], 112). Pentru prezentări ale cazului de spionaj respectiv, vezi Robert Lindsey, The Falcon and the Snowman (New York: Simon and Schuster, 1979) şi Curtis Peebles, Guardians: Strategic Reconnaissance Satellites (Novato, Calif.: Presidio, 1987), 200 – 201.

23. Dino Brugioni, el însuşi un fost PI, subliniază acest aspect în prezentarea pe care a făcut-o în cadrul unei informări extrem de importante din timpul crizei rachetelor cubaneze. El menționează că persoana care a interpretat pentru prima dată fotografia şi care l-a informat pe Kennedy a înțeles că importanța fotografiilor cu locațiile rachetelor era mai mult decât evidentă şi s-a străduit să îl îndrume pe preşedinte pe parcursul analizei PI – iar în final, Kennedy a

întrebat: "Sunteți sigur?" Brugioni, Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis (New York: Random House, 1991), 230.

24. "Rezoluția la sol" se referă la capacitatea fotografiei de a reda un șablon standard abia distinct alcătuit din linii paralele în alb și negru (adică linii și spații) de aceeași lățime. O distanță a rezoluției la sol, de exemplu de un picior (30,48cm) ar genera o fotografie în care șablonul având lățimea liniilor și spațiilor de un picior este greu de distins. Un șablon mai de dimensiuni mai reduse, cu o lățime mai mică a liniilor și spațiilor, nu s-ar mai distinge deloc. (Această definiție și citatul din text sunt din Amrom Katz, "Observation Satellites: Problems and Prospects," Astronautics [Aprilie 1960]: 5 – 6, o discuție "în esență identică" cu cea a lui Amrom Katz, Observation Satellites: Problems, Possibilities and Prospects, RAND Paper P – 1707 [Santa Monica, Calif.: RAND, 25 mai 1959].)

25. Pentru o listă a rezoluțiilor la sol necesare pentru efectuarea analizei foto la diferite niveluri destinate mai multor tipuri de ținte, vezi Amron Katz, "Technical Collection," în Intelligence Requirements for the 1980s: Clandestine Collection, ed. Roy Godson (Washington, D.C.: National Strategy Information Center, 1982), 109.

26. Pentru o listă cu elementele de bază care se utilizează la elaborarea unei semnături, vezi Brugioni, Eyeball to Eyeball, 196.

27. Pentru o discuție legată de cratologie, vezi Robert S. Greenberger, "Can CIA Cratology Ultimately Outsmart Kremlin's Shellology?" Wall Street Journal, 10 ianuarie 1985, A1.

28. Brugioni, Eyeball to Eyeball, 104 – 105, 276 – 77.

29. Brugioni, Eyeball to Eyeball, 538 – 48.

30. Robin Wright, "US Intelligence Failed to Warn of India's Atom Tests," Los Angeles Times, 13 mai 1998, A1 și James Risen și Tim Weiner, "US May Have Helped India Hide Its Nuclear Activity", New York Times, 25 mai 1998, A3.

31. Sherman Kent, Strategic Intelligence for American World Policy (Princeton, N.J.: Princeton University Press, 1949; re-editată, 1966), 12 – 13, oferă cuprinsul unei cărți referitoare la o țară de interes, redactată în Germania pentru a fi utilizată în timpul celui de-al Doilea Război Mondial:

    I. Condiții generale. Locație. Frontiere. Zonă. Istorie. Structură guvernamentală și administrativă.

    II. Caracteristicile țării. Forme de relief. Soluri. Suprafața terenului. Climat. Aprovizionarea cu apă.

    III. Poporul. Naționalități. Limbă. Atitudini. Distribuția populației. Așezări. Sănătate. Structura societății.

    IV. Economia. Agricultură. Industrie. Afaceri și Comerț. Exploatări miniere. Pescuit.

    V. Transporturile. Căi ferate. Drumuri. Porturi. Aeroporturi. Căi navigabile fluviale.

    VI. Geografia militară. [Delimitare detaliată pe regiuni].

    VII. Sistemul militar actual. Armata: ordinea de luptă; sisteme fixe de apărare, echipamente militare, aprovizionare. Flota militară: ordinea de luptă,

flota, echipamente maritime de coastă, spaţiul aerian maritim, aviaţia militară: ordinea de luptă, flota aeriană militară, echipamente de zbor mai uşoare decât aerul, aprovizionare.

VIII. Anexe speciale. Date biografice referitoare la membri importanţi ai guvernului. Terminologie geografică locală. Descrierea râurilor, lacurilor, canalelor. Listă şi caracteristici ale centralelor electrice. Descrierea drumurilor. Listă cu aerodromurile şi principalele piste de aterizare. Listă cu principalele linii telefonice şi de telegraf. Bani, unităţi de măsură. Plaje [pentru operaţiuni militare derulate cu amfibii].

32. Camera Reprezentanţilor, Comisia pentru Forţele Armate, Lessons Learned as a Result of the US Military Operations in Grenada: Hearing, Congresul 98, şedinţa a doua, 1984, H. Rept. 98 – 43, 24. Având în vedere faptul că administraţia Reagan şi-a exprimat în mod expres îngrijorarea provocată de regimul marxist – leninist din Grenada, condus de Maurice Bishop (a cărui arestare şi execuţie de către colegii săi a declanşat evenimentele şi apoi invazia), această lipsă a hărţilor şi a altor date importante reprezintă un exemplu de eşec în anticiparea politicii SUA.

33. Pentru o discuţie completă privind această sarcină, prezentată drept o evitare a surprizelor rezervate de tehnologie, vezi Michael I. Handel, "Technological Surprise in War", Intelligence and National Security 2, nr. 1 (ianuarie 1987): 1 – 53. Handel caracterizează în felul următor importanţa informaţiilor secrete ştiinţifice şi tehnice:

Mai mult decât oricare război anterior, războiul modern, care are la bază dezvoltarea continuă a noilor sisteme de armament într-un ritm din ce în ce mai accelerat, depinde de informaţiile secrete… Chiar şi înainte de începerea luptei, deseori "bătălia informaţiilor secrete" a decis cine a ieşit învingător şi cine a pierdut. Rolul pe care-l deţin informaţiile secrete ştiinţifice tehnologice în război va creşte proporţional cu evoluţia tehnologică a inamicilor şi cu modul în care aceştia utilizează armamentul de ultimă oră. [pag.40].

34. R. V. Jones, The Wizard War: British Scientific Intelligence, 1939 – 45 (New York: Coward, McCann şi Geoghegan, 1978), 104. Sistemul Knickebein presupunea două atene care transmiteau fascicule radio unidirecţionale ce se intersectau deasupra ţintei bombardierelor; bombardierele germane zburau de-a lungul unui fascicul şi-şi lansau bombele când se intersectau cu celălalt. După ce au aflat de existenţa acestui sistem şi i-au stabilit caracteristicile, britanicii au iniţiat măsuri de contracarare a acestuia – bruiaj şi lansarea de fascicule false - care i-au diminuat eficienţa în mod semnificativ şi le-au zădărnicit trupelor germane eforturile de a efectua operaţiuni de bombardare a unor ţinte precise din Marea Britanie (127 – 128).

35. Eliot Cohen, "Analysis", în Intelligence Requirements for the 1990s: Collection, Analysis, Counterintelligence and Covert Action, ed. Roy Godson (Lexington, Mass.: Heath, Lexington, 1989), 82.

36. Jan Karl Tanenbaum, "French Estimates of Germany's Operational War Plans", în Knowing One's Enemies: Intelligence Assessment before the Two World Wars, ed. Ernest May (Princeton, N.J.: Princeton University Press, 1984), 150 – 71.

37. Lucrurile nu au stat neapărat aşa nici în cazul economiei sovietice, care permitea accesul analiştilor din serviciile secrete la date nepublicate, ce le-ar fi

putut oferi acestora un avantaj faţă de alţi experţi. De exemplu, în 1977, CIA a redactat o serie de studii privind industria petrolieră sovietică, iar acestea au anticipat că, până în 1985, producţia va scădea la opt – zece milioane de barili pe zi, iar Uniunea Sovietică va importa între 3,5 şi 4,5 mb/zi. Experţii din mediul academic şi din cel de afaceri s-au arătat sceptici faţă de aceste rezultate, care într-adevăr, s-au dovedit a fi departe de realitate. În anii 1980, producţia de petrol sovietic a stagnat sau s-a apropiat de 12 mb/zi. Pentru o analiză a acestei chestiuni care a stârnit simpatia generală faţă de CIA, vezi Senatul SUA, Comisia Specială pentru Serviciile de Informaţii, The Soviet Oil Situation: An Evaluation of CIA Analyses of Soviet Oil Production: Staff Report, Congresul 95, şedinţa a doua, 1978, Committee Print. Pentru o analiză critică a activităţii derulate de serviciile americane de informaţii pentru a evalua pe ansamblu economia fostei Uniuni Sovietice, vezi Senatul SUA, Comisia pentru Relaţii Externe, Estimating the Size and Growth of the Soviet Economy: Hearing, Congresul 101, şedinţa a doua, 1990, S. Hrg. 101 – 1112.

38. Kent, Strategic Intelligence, 7 – 8.

39. Uneori, serviciile de informaţii sunt văzute ca fiind concurenţi ai presei, ceea ce este deseori în dezavantajul acestora. De exemplu, comunicatele de presă care anunţau că funcţionarii americani au urmărit lovitura de stat panameză din octombrie 1989 la CNN, au insinuat că acest lucru era o dovadă a eşecului serviciilor de informaţii americane. Este o comparaţie incorectă, întrucât CIA nu are sarcina de a furniza rapoarte de ultimă oră. Se pare că această critică a avut un oarecare impact. Vezi George Lardner Jr., "On This Network, All the News Is Top Secret: Defense Intelligence Agency Acts to Win Back Audience from CNN," Washington Post, 3 martie 1992, A1 şi George Lardner Jr. şi Walter Pincus, "Clearance Sought for New CIA Network: Agency Would Transmit Latest Intelligence Only to Select Top Officials," Washington Post, 5 februarie 1992, A1.

40. Kent, Strategic Intelligence, 38.

41. Adresa web al Directoratului CIA privind informaţiile secrete (accesat pe 10 martie 2001) ***www.odci.gov/cia/di/work/daily.html***.

42. Cord Meyer, Facing Reality, From World Federalism to the CIA (New York: Harper and Row, 1980), 352. Fostul DCI Robert Gates scria, în 1989:

    De la un preşedinte la altul, PDB a cunoscut puţine modificări: câteva telegrame (între trei şi şase) ale DoS (Departamentul de Stat) şi ale CIA de importanţă deosebită; ocazional, un raport cu informaţii secrete de la CIA, de la DIA sau de la NSA; anumite servicii prin cablu, rapoarte (rare) privind situaţia DoS şi CIA, în cazul crizelor din alte ţări şi dese telegrame cuprinzând informări matinale aparţinând NSC şi DoS.

    Din perspectiva lui Gates, adevărata schimbare radicală în activitatea curentă de informaţii a constat în înfiinţarea de către administraţia Kennedy a Biroului pentru situaţii de criză al Casei Albe, la începutul anilor 1960. Anterior, "preşedintele se afla la mila aparatului birocratic pe probleme de informaţii." Prin înfiinţarea Biroului pentru situaţii de criză, Departamentul de Stat, Departamentul pentru Apărare, CIA şi NSA au început să le comunice preşedintelui şi echipei sale "informaţii secrete neevaluate sau brute, pe cale electronică." Gates apreciază că această inovaţie a avut ca rezultat "diminuarea semnificativă a numărului de rapoarte informative înaintate Casei Albe de către

CIA şi alte servicii de informaţii." Robert Gates, "An Opportunity Unfulfilled: The Use and Perceptions of Intelligence at the White House," The Washington Quarterly 12, nr. 1 (iarna 1989): 37.

43. Adresa de web a Directoratului CIA privind informaţiile secrete. Pentru a ilustra atenţia acordată de administraţia Clinton aspectelor economice ale problematicii internaţionale, începe să se publice Economic Executives' Intelligence Brief (EEIB), cel de-al treilea cotidian care acoperă "aspecte problematice din activitatea directorilor economici, cum ar fi proceduri ale comerţului exterior, finanţări ilicite şi evoluţia unor companii energetice pe plan internaţional."

44. Senatul SUA, Comisia Specială pentru Evaluarea Operaţiunilor Guvernamentale legate de Activităţile de Culegere de Informaţii [de aici înainte de va numi Comisia Church], Final Report, vol. 1: Foreign and Military Intelligence, Congresul 94, şedinţa a doua, 1976, S. Rept. 94 – 755, 272 – 73.

45. Aveţi în vedere următoarea observaţie a unui înalt funcţionar al Departamentului de Stat SUA: "Ieri a venit la mine un prieten de-al meu din CIA să-mi dea o informare privind Germania de Est. Mi-a spus că şi-a citit materialul de trei ori din cauza a ceea ce a auzit la radio, în timp ce se afla în maşină, pe drum, dinspre CIA către Departamentul de Stat." (Thomas L. Friedman, "In Quest for a Post – Cold War Plan," New York Times, 17 noiembrie 1989, A22). Această remarcă a demonstrat cât de rapide au fost transformările suferite de Europa de Est în noiembrie 1989, cât şi faptul că raportul analistului s-a axat în special pe cele mai recente evenimente şi mai puţin pe înţelegerea profundă a dinamicii politice din Germania de Est.

46. Pentru o prezentare completă a analizei avertismentelor, vezi Timothy M. Laur, "Principles of Warning Intelligence," în The Military Intelligence Community, ed. Gerald W. Hopple şi Bruce W. Watson (Boulder, Colo.: Westview, 1986), 149 – 68.

47. Gordon Brook – Shepherd, Storm Birds: Soviet Postwar Defectors (New York: Weidenfeld and Nicolson, 1989), 330 – 31, şi Christopher Andrew şi Oleg Gordievsky, editori, Instructions from the Centre: Top Secret Files on KGB Foreign Operations, 1975 – 1985 (Londra: Hodder and Stoughton, 1991), 67 – 90.

48. Conform ultimului ordin executiv privind activităţile serviciilor de informaţii din SUA (EO 12333, 4 decembrie 1981), "comunitatea serviciilor de informaţii" cuprinde CIA, NSA, DIA, "birouri din cadrul Departamentului Apărării care culeg informaţii secrete externe specializate prin intermediul programelor de recunoaştere", Biroul pentru Culegere de Informaţii şi Cercetare din cadrul Departamentului de Stat (INR) şi departamentele de culegere a informaţiilor din cadrul armatei, FBI şi Departamentele Trezorerie şi Energie (paragr. 3.4 [f]). Textul ordinului executiv este disponibil la adresa de web a Arhivelor Naţionale, ***www.nara.gov/fedreg/codific/eos/e12333.html***.

49. Avi Shlaim, "Failures in National Intelligence Estimates: The Case of the Yom Kippur War," World Politics 28, nr. 3 (aprilie 1976): 368 – 369.

50. Alexander Orlov, Handbook of Intelligence and Guerilla Warfare (Ann Arbor: University of Michigan Press, 1965), 10. Cunoscând, se pare, sistemul american, după cel de-al Doilea Război Mondial, Stalin a înfiinţat un birou unic de evaluare a informaţiilor secrete. Cu toate acestea, având în vedere instrucţiunile şi comportamentul anterior al lui Stalin, era de aşteptat ca biroul

respectiv să nu aibă acces la toate informaţiile, iar analizele sale să reflecte ceea ce dorea acesta să audă. (V. M. Zubok, "Soviet Intelligence and the Cold War: The 'Small' Committee of Information, 1952 – 1953," Lucrarea a 4-a a Proiectului privind Istoria Războiului Rece [Washington, DC: Woodrow Wilson Center, 1992]). Comisia s-a desfiinţat în 1958. În ansamblu, există puţine materiale disponibil epublicului cu privire la procesele de evaluare din alte ţări, cu excepţia Statelor Unite. Totuşi, pentru o prezentare amplă a sistemului britanic şi a istoriei sale organizatorice, vezi Reginald Hibbert, "Intelligence and Policy", Intelligence and National Security 5, nr. 1 (ianuarie 1990): 110 – 27 şi Michael Herman, "Intelligence and Policy: A Comment," Intelligence and National Security 6, nr. 1 (ianuarie 1991): 229 – 39.

51. Barton Whaley, Codeword Barbarossa (Cambridge: MIT, 1973); Shlaim, "Failures in National Intelligence Estimates," 348 – 80; Michael I. Handel, Perception, Deception and Surprise: The Case of the Yom Kippur War (Jerusalem: Leonard Davis Institute for International Relations, Jerusalem Paper 19, 1976); Eliot Cohen şi John Gooch, Military Misfortunes: The Anatomy of Failure in War (New York: Free Press, 1990), cap. 5 ("Failure to Anticipate: Israeli Defence Forces on the Suez Front and the Golan Heights, 1973"), 95 – 131; Roberta Wohlstetter, Pearl Harbor: Warning and Decision (Stanford, Calif.: Stanford University Press, 1962), Edwin T. Layton, "And I Was There": Pearl Harbor and Midway – Breaking the Secrets (New York: Morrow, 1985); Gordon W. Prange et. Al., At Dawn We Slept: The Untold Story of Pearl Harbor (New York: McGraw – Hill, 1981) şi, în general, Klaus Knorr şi Patrick Morgan, eds. Strategic Military Surprise: Incentives and Opportunities (New Brunswick, N.J.: Transaction, 1983).

52. Vezi Harvey de Weerd, "Strategic Surprise in the Korean War," Orbis 6, nr. 3 (toamna lui 1962): 435 – 52 şi Eliot Cohen, " 'Only Half the Battle': American Intelligence and the Chinese Intervention in Korea, 1950", Intelligence and National Security 5, nr. 1 (ianuarie 1990): 129 – 49. În legătură cu ofensiva din Ardeni, vezi Charles B. MacDonald, A Time for Trumpets: The Untold Story of the Battle of the Bulge (New York: Morrow, 1985), 17 – 92 şi Hinsley et. al., British Intelligence in the Second World War, vol. 3, pt. 2, 402 – 38. Pentru ofensiva Tet, vezi James J. Wirtz, The Tet Offensive: Intelligence Failure in War (Ithaca, N.Y.: Cornell University Press, 1991).

53. Lewin, Ultra Goes To War, 317 – 18.

54. La momentul respectiv, acest eşec a fost considerat suficient de distructiv pentru ca preşedintele Carter să adreseze o notă de mână către Cyrus Vance, Zbigniew Brzazinski şi Stansfield Turner (secretar de stat, consilier prezidenţial pe probleme de securitate naţională şi respectiv director al serviciului central de informaţii), în care a specificat, cu o franchețe necaracteristică birocraţiei guvernamentale: "nu sunt mulţumit de calitatea rapoartelor noastre politice." Stansfield Turner, Secrecy and Democracy: The CIA in Transition (Boston: Houghton Mifflin, 1985; New York: Harper and Row, 1986), 113. Vezi şi Camera Reprezentanţilor, Comisia permanentă pe probleme de informaţii, Sub-comisia de Evaluare, Iran: Evaluation of US Intelligence Performance prior to November 1978: Staff Report, Congresul 96, şedinţa 1, 1979.

55. Un raport al Comisiei Senatului SUA privind serviciile de informaţii susţine că "problema nivelurilor preţului petrolului a fost analizată în cadrul restrâns cerere

– ofertă, care tindea să amplifice atât influenţele politice, cât şi anumiţi factori economici, cum ar fi flexibilitatea cererii şi a ofertei." Raportul pretinde şi că "aspectele politice ale relaţiilor dintre statele membre OPEC şi dinamica internă a guvernului saudit… nu au fost integrate în mod consecvent în evaluarea economică a comunităţii" (Comisia Specială pentru Serviciile de Informaţii, Subcomisia de analiză a activităţii de culegere, producere şi a calităţii informaţiilor secrete, US Intelligence Analysis and the Oil Issue, 1973-1974: Staff Report, Congresul 95, şedinţa 1, 1977, Committee Print, 4, 5). Aceasta sugerează că analiştii pe probleme de securitate implicaţi au elaborat o analiză economică prea teoretică şi, în consecinţă, apolitică.

56. Campania peninsulară din timpul Războiului Civil, condusă de generalul George McClellan în primăvara şi vara anului 1862, reprezintă un exemplu clasic de eşec al serviciilor de informaţii. McClellan şi-a mutat armata unională alcătuită din 85.000 de combatanţi pe cale maritimă, din Washington în peninsula formată de râurile James şi York din Virginia. El intenţiona să avanseze în interiorul peninsulei şi să ocupe Richmond (capitala Confederaţiei), încheind astfel războiul. Cu toate acestea, la Yorktown, McClellan s-a lovit de rezistenţa Confederaţiei. Pe baza informaţiilor secrete furnizate în mare parte de celebrul detectiv particular Allan Pinkerton, McClellan a crezut că va înfrunta un inamic redutabil; de fapt, era vorba despre 17.000 de soldaţu ai Confederaţiei, dispuşi pe un front de opt mile. În loc să atace şi să spargă frontul Confederaţiei, McClellan a preferat asediul de lungă durată, care a oferit Sudului timp suficient pentru a se regrupa.

    În primăvară şi în vară, atât armata unională, cât şi cea a Confederaţiei, şi-au sporit efectivele. Dar încă o dată, bazându-se pe informaţii secrete incorecte, Mc Clellan a fost sigur că se confruntă cu o armată a sudiştilor formată din 200.000 de combatanţi; de fapt, era vorba de numai trei sferturi din propria sa armată de 112.000 de soldaţi. În august, crezând că este cu mult depăşit din punct de vedere numeric, generalul McClellan a abandonat campania şi prin aceasta şansa optimă de a obţine o posibilă victorie rapidă asupra Sudului. Vezi C.T. Schmidt, "G-2, Army of the Potomac," Military Review 28 (iulie 1948), 45 – 56 şi Edwin C. Fishel, "Pinkerton and McClellan: Who Deceived Whom?" Civil War History 34, nr. 2 (iunie 1988), 115 – 42.

    Un alt exemplu mai concludent este al lui Williamson Murray, care a argumentat că evaluările defectuoase realizate de Franţa şi Marea Britanie în ceea ce priveşte echilibrul de forţe din Europa în perioada 1938 – 39 au făcut ca aceste două ţări să nu fructifice momentele avantajoase de atunci, pentru a obţine o victorie mai puţin costisitoare (comparativ cu ceea ce a urmat) împotriva Germaniei naziste. Williamson Murray, The Change in the European Balance of Power, 1938 – 1939: The Path to Ruin (Princeton University Press, 1984).

57. Au existat elemente de surpriză tactică, de exemplu, în dispunerea de către Aliaţi a porturilor artificiale, care să se utilizeze până la capturarea unor porturi importante, cum ar fi Cherbourg. Vezi Handel, "Technological Surprise in War", 14 – 15, pentru o dezbatere pe problema pe care o reprezentau aceste porturi artificiale pentru serviciile de informaţii germane.

58. Vezi Cohen, "Only Half the Battle." Cohen susţine că deşi este posibil ca atacul chinezilor să fi luat prin surpindere conducerea politică de la Washington, generalul MacArthur, comandantul armatei SUA şi al trupelor

ONU, ştia despre infiltrarea masivă a trupelor chineze în Coreea; dezastrul nu a fost provocat atât de surpriză, cât de aplicarea tacticilor necorespunzătoare împotriva armatei chineze. Generalul MacArthur a crezut că SUA puteau să profite de supremaţia deţinută în atacurile aeriene şi în lupta sa împotriva Armatei de Eliberare a Poporului Chinez (PLA), cât şi împotriva Armatei Poporului Nord Koreean (NKPA). În cele din urmă, această opinie eronată a reflectat o greşeală de evaluare a diferenţelor dintre NKPA-ul bine echipat din punct de vedere tehnic şi deci limitat la deplasarea rutieră (construit după modelul sovietic) şi PLA-ul fără echipamente mecanizate, ale cărui trupe dispersate de infanterie nu au constituit ţinte eficiente pentru atacurile aeriene.

59. Lewin, Ultra Goes to War, 347 – 51.

60. John Prados, The Soviet Estimate: US Intelligence Analysis and Russian Military Strength (New York: Dial, 1982), 41 – 50, 76 – 95, 111 – 26.

61. Albert Wohlstetter, "Is There A Strategic Arms Race?" Foreign Policy, nr. 15 (vara anului 1974): 3 – 20 şi "Rivals, but not Race," Foreign Policy, nr. 16 (toamna anului 1974); 48 – 81.

62. De exemplu, Donald Rumsfeld, care în 1998 a devenit preşedintele Comisiei de Evaluare a Ameninţărilor cu Rachete Balistice asupra Statelor Unite, a susţinut că un NIE anterior a subestimat ameninţarea respectivă pentru că, printre altele, analiştii care s-au ocupat de acest subiect nu au avut acces la informaţiile privind transferul de tehnologie între diferite state. În consecinţă, evaluarea lor privind perioada în care anumite state vor construi rachete balistice capabile să atace Statele Unite a avut la bază perioada de timp în care respectivele state vor putea construi tehnologie cu resurse interne. Întrucât a avut acces la informaţii privind transferul de tehnologie, Comisia a ajuns la concluzia că unele dintre aceste ţări ar putea reprezenta în scurt timp o ameninţare împotriva Statelor Unite din cauza deţinerii de rachete balistice. Eric Schmitt, "Panel Says US Forces Risk a Surprise Missile Attack," New York Times, 16 iulie 1998, A24 şi The News Hour with Jim Lehrer, 15 iulie 1998, interviu cu Donald Rumsfeld.

63. Norman Schwarzkopf, It Doesn't Take a Hero: The Autobiography (New York: Bantam, 1992), 293; Bob Woodward, The Commanders (New York: Simon and Schuster, 1991), 205 – 208, 215 şi Bruce W. Jensen, With Friends Like These: Reagan, Bush and Saddam, 1982 – 1990 (New York: Norton, 1994), 173 – 74.

64. Wesley K. Wark, The Ultimate Enemy: British Intelligence and Nazy Germany, 1933 – 1939 (Ithaca, N.Y.: Cornell University Press, 1985), 228 – 29.

65. Acest aspect este similar problemei legate de „modificarea paradigmei" abordată în filozofia ştiinţei – adică felul în care un cadru de organizare, precum fizica newtoniană, dă naştere altui cadru de organizare (de exemplu, relativitatea). Cu toate acestea, trebuie evidenţiate două diferenţe importante, care sugerează că modificarea paradigmei poate avea loc mai uşor atunci când este vorba despre o teorie ştiinţifică decât atunci când este vorba despre analiza informaţiilor secrete: (1) pionierii noilor idei nu au nevoie nici măcar de îngăduinţa, cu atât mai puţin de acordul adepţilor vechilor concepţii pentru a-şi publica opiniile, şi (2) se pot elabora şi efectua experimente special concepute pentru a se adopta una dintre cele două variante de concepţii. Chiar şi aşa, unii au pretins că modificările nu sunt atât rezultatul adoptării noilor idei de către

oamenii de știință aflați deja în domeniu, cât al adoptării acestora de către noii veniți în disciplina respectivă.

66. Uneori, acest mecanism este desemnat de termenul „proiecție", specific domeniului psihologiei, care în sens mai tehnic, înseamnă mecanismul psihologic prin care un subiect atribuie altui subiect sentimente sau caracteristici (precum ostilitatea și reaua-credință) pe care nu le agreează la propria persoană și pe care vrea să le renege. Întrucât în anumite cazuri, acest mecanism poate reprezenta baza psihologică a imaginii în oglindă, cele două concepte, care acționează la nivele diferite, nu sunt identice; de exemplu, proiecția nu poate fi cauza atribuirii eronate, către un inamic, a unei caracteristici (cum ar fi împăcarea și mulțumirea față de status quo) pe care o are și de care este mulțumit.

67. Eșecul serviciilor de informații israeliene în acest caz este abordat în Shlaim, „Failures in National Intelligence Estimates." Shlaim opinează că în fața probelor privind un potențial atac, serviciile de informații israeliene au avut în continuare „concepția" sau ideea că Egiptul nu va ataca până când nu va fi capabil să organizeze atacuri aeriene ample pentru a distruge forțele aeriene israeliene, iar Siria nu va ataca fără Egipt. Prima și cea mai importantă parte a acestei concepții reflectă, la nivel militar, aceeași imagine în oglindă existentă la nivel politic – credința că Egiptul nu va începe un război pe care nu are șanse reale să-l câștige. Totuși, în analiza lor referitoare la războiul din 1973 (Military Misfortunes, cap. 5), Cohen și Gooch susțin că această „concepție" nu s-a bazat doar pe perspectiva imaginii în oglindă. Israel a avut probe relativ recente și direct referitoare la evaluarea făcută de Egipt cu privire la resursele necesare pentru a câștiga războiul cu Israelul (116). Prin urmare, în acest caz, eșecul analitic nu a pornit de la perspectiva imaginii în oglindă la nivel militar, ci de la imposibilitatea de a se preconiza că Egiptul și-ar putea modifica noțiunea de succes strategic (succes cu privire la obiectivele politice generale ale unui război, 123 – 24). Acest eșec pare să indice o imagine în oglindă la nivel politic.

68. Al – Hamishmar, 14 septembrie 1975, așa cum a fost citat în Shlaim, „Failures in National Intelligence Estimates," 362.

69. Acest pasaj a fost șters din versiunea finală a NIE, dar a continuat să existe sub forma unei note de subsol care exprima opiniile diferite ale directorului INR din cadrul Departamentului de Stat. Comisia Church, Final Report, vol. 1, 78. Textul complet al NIE este disponibil în Donald Steury, ed., Intentions and Capabilities, Estimates on Soviet Strategic Forces, 1950 – 1983 (Washington, DC: Center for Study of Intelligence, CIA, 1996), 253 – 61. Nota de subsol apare la pagina 261.

70. Jones, The Wizard War, 457.

71. Jones, The Wizard War, 458. Evoluțiile înregistrate de tehnologia radar înaintea celui de-al Doilea Război Mondial oferă două exemple interesante de eșec al evaluării diferențelor dintre abordarea inamicului privind o anumită problemă tehnică și abordarea proprie. La mijlocul anilor 1930, atât Marea Britanie cât și Germania demonstraseră că detectarea la distanță a avioanelor s-a putut realiza prin utilizarea transmisiilor radio (radar). Cu toate acestea, niciuna dintre aceste două țări nu a știut că cealaltă a aflat „secretul" radarului, deși amândouă realizaseră și puseseră în practică sistemele până în 1939. În

absența detectării unei transmisii radar germane, Comunitatea tehnică și de informații britanică a respins toate probele (fotografice sau umane) cum că Germania ar fi deținut radare. Nu s-a detectat niciun semnal întrucât Germania inventase radare cu mult diferite de cele britanice. În multe privințe, radarele germane erau mai bune, dar aveau un defect: rază de acțiune limitată. Ca urmare, semnalele radar nu au fost detectate în Marea Britanie doar pentru că erau prea slabe pentru a fi detectate de la distanță mare.

Comunitatea specialiștilor germani în domeniul tehnicii era mai puțin convinsă decât comunitatea britanică de faptul că doar radarul în sine constituia „o minune a tehnicii". În consecință, germanii s-au străduit să capteze semnale ale britanicilor. Întrucât căutau un semnal similar cu al lor, au stabilit în mod eronat că semnalele radar captate de ei proveneau de la rețeaua britanică de curent electric; de fapt, britanicii nu fuseseră capabili să producă un semnal atât de performant și concepuseră unde radar diferite, dar tot eficiente. Din cauza acestei erori de analiză, Luftwaffe nu a produs echipamentul necesar pentru a contracara la timp radarele britanice în Bătălia Angliei, oferind astfel Forțelor Aeriene Regale un avantaj semnificativ în spațiul aerian al Marii Britanii. Jack Nissen, cu A.W. Cockerill, Winning the Radar War (Londra: Robert Hale, 1989), 17 – 39 și Jones, The Wizard War, 189 – 202.

72. În principiu, putem vorbi despre eșecuri în culegerea informațiilor secrete; cu toate acestea, rareori auzim de ele, mai ales întrucât cele mai interesante cazuri sunt cele în care informațiile de interes erau de fapt disponibile.

73. În măsura în care serviciile de informații se preocupă mai puțin de aspectele politice și militare și mai mult de cele economice și sociale (cum a sugerat, de exemplu, William Colby, fostul director CIA și după cum s-a discutat în Capitolul 7), această afirmație este mai puțin convingătoare. Un serviciu de informații care se ocupă în special de elaborarea prognozelor socio-economice poate descoperi că adversarii săi nu sunt interesați de progresele înregistrate de serviciu și nu doresc să-l obstrucționeze în vreun fel. (Dar nu neapărat: în anii 1920, sovieticii s-au străduit să convingă serviciile de informații occidentale că în Uniunea Sovietică, comunismul dispare, iar liderii acestuia adoptă un naționalism inofensiv. John J. Dziak, Chekistry: A History of the KGB [Lexington, Mass.: Heath, Lexington, 1988], 48.)

În mod similar, uneori se vrea ca inamicul să înțeleagă situația în mod corect. De exemplu, strategia de constuire a unui scut de arme nucleare (presupunând că un stat dispune de forțele necesare pentru a o pune în practică și că nu este vorba despre un bluf) depinde de evaluarea corectă făcută de către un alt guvern, care stabilește că după primul atac, armata respectivă va mai putea provoca pagube imense țării sale. Așa s-a întâmplat în toamna și iarna anului 1961, când printr-o serie de discursuri și articole de ziare, înalți funcționari din administrația Kennedy le-au comunicat în mod intenționat sovieticilor că SUA nu mai are nicio îndoială cu privire la superioritatea sa în domeniul armamentului nuclear. Bazându-se pe capacitatea sa de a „descifra" secretele armatei sovietice, guvernul american știa că nu mai exista nicio „diferență în ceea ce privește rachetele" și că deține arme mai mult decât suficiente pentru a declanșa a doua ofensivă devastatoare împotriva URSS-ului, în eventualitatea izbucnirii războiului. Vezi Prados, The Soviet Estimate, 172.

74. Senatul SUA, Comisia Specială pentru Serviciile de Informaţii, Sub-comisia privind culegerea, producerea şi calitatea informaţiilor secrete, The National Intelligence Estimates A – B Team Episode Concerning Soviet Strategic Capability and Objectives, Congresul 95, şedinţa a doua, 1978, Committee Print. (Partea din raportul echipei A – B privind intenţiile strategice ale sovieticilor a fost publicată în 1992 într-o formă revizuită de CIA.)

75. Mandatul Congresului de înfiinţare a comisiei bipartite a survenit după două evaluări prealabile ale NIE, ambele considerând că analiza cuprinsă în NIE este defectuoasă. Senatul SUA, Comisia Specială pentru Serviciile de Informaţii, Hearing on Intelligence Analysis on the Long – Range Missile Threat to the United States, 4 decembrie 1996, disponibil la adresa www.fas.org.irp/congress/1996_hr /index.html; "Foreign Missile Threats: Analytic Soundness of Certain National Intelligence Estimates," GAO Letter Report (GAO/NSAID-96-225), 30 august 1996, disponibil la ***www.fas.org/irp/gao/nsi96225.htm;*** şi Report of the Commission to Assess the Ballistic Missile Threat of the United States, 15 iulie 1998, disponibil la adresa ***www.fas.org/irp/threat/bm-threat.htm***.

76. Potrivit lui Shlomo Gazit, serviciile militare secrete israeliene se folosesc în mod curent de un "avocat al diavolului" în eforturile de încurajare a unei atitudini mai deschise în procesul analitic. Shlomo Gazit, "Estimates and Fortune-Telling in Intelligence Work," *International Security* 4, no. 4 (primăvara anului 1980): 40, n. 3.

În anul 1985, Statele Unite au folosit o abordare tipică "avocatului diavolului" pentru a reanaliza problema complicităţii sovietice la încercarea de asasinare a Papei Ioan Paul al II-lea din anul 1981. În perioada imediat următoare atacului, CIA era de părere că tentativa de asasinare trebuia pusă pe seama unui singur individ. În 1985, conform unor noi informaţii, ţinute secrete până în acel moment, era posibil ca Bulgaria şi Uniunea Sovietică să fi fost implicate în atacul împotriva Papei; astfel, Robert Gates, adjunctul Directorului Agenţiei Centrale de Informaţii, a ordonat elaborarea unei evaluări în stilul tipic "avocatului diavolului" pentru a aduce argumente în favoarea implicării Uniunii Sovietice. Această evaluare a fost folosită în timpul audierilor de către cei care se opuneau nominalizării lui Gates, drept exemplu pentru presupusa lui disponibilitate de a modifica o analiză astfel încât aceasta să corespundă opiniilor generale ale membrilor administraţiei. După cum sugerează această controversă (precum şi exerciţiul Echipei A-B care s-a desfăşurat înaintea acesteia), încercarea de a folosi o abordare tipică "avocatului diavolului" pentru analiza unui singur aspect poate fi foarte uşor criticată ca fiind un efort de a politiza analizele realizate de serviciile secrete. Senatul Statelor Unite, Comisia specială privind activitatea serviciilor secrete, *Nomination of Robert Gates to be Director of Central Intelligence: Hearings*, 102d Cong., prima sesiune, 1991, S. Hrg. 102-799: vol. 1, 637; vol. 2, 347 ff. şi 619; vol. 3, 62-118. Benjamin Weiser, "Papal-Shooting Analysis: Case Study in Slanting?" *Washington Post*, 1 octombrie 1991, A8.

Comisia Rumsfeld s-a format în urma unei controverse referitoare la utilizarea de către Statele Unite a unui sistem de apărare împotriva rachetelor balistice. Totuşi, Comisia a scăpat de acuzaţia de politizare, deoarece membrii acesteia

(printre care se numărau experţi ai ambelor tabere) au căzut de acord, în mod unanim, asupra raportului final. Comisia a fost ajutată şi de faptul că, la scurt timp după emiterea raportului din iulie 1998, Coreea de Nord a lansat o rachetă considerată a fi capabilă să lovească Alaska sau Hawaii.

77. Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31, nr. 1 (octombrie 1978): 61-89.

CAPITOLUL 4
ÎN CULISE: OPERAȚIUNILE SECRETE

1. Legea privind autorizarea activității serviciilor de informații, anul fiscal 1991, L. 102-88, 14 august 1991 [50 USC 413b].
2. Activitățile secrete au fost "definite" pentru prima dată în 1974 prin Amendamentul Hughes-Ryan (Secțiunea 662 din Legea privind asistența externă din 1961, [22 USC 2242]). Acest act normativ nu oferea o definiție în sensul strict al cuvântului; dar le cerea președinților să autorizeze în mod explicit, și apoi să raporteze Congresului, toate "operațiunile [inclusiv cheltuielile realizate de către sau în numele CIA] efectuate în state străine, altele decât cele care au ca scop obținerea de informații secrete." Până în 1991, definirea activităților secrete (sau a "acțiunilor speciale", după cum mai sunt numite) a fost lăsată spre a fi interpretată ulterior în decretele și directivele prezidențiale emise de comisiile de supraveghere ale Congresului. Pentru o sinteză a evoluției definiției acțiunilor sub acoperire anterioare anului 1991, consultați Americo R. Cinquegrana, "Dancing in the Dark: Accepting the Invitation to Struggle in the Context of "Covert Action," the Iran-Contra Affair and the Intelligence Oversight Process," *Houston Journal of International Law* 11, nr. 1 (toamna anului 1988): 177-209.
3. John Bruce Lockhart, fost reprezentant al Ministerului de Externe britanic cu o experiență vastă în domeniul serviciilor secrete, folosește termenul de "acțiune politică specială" ca sinonim pentru acțiunile secrete; această expresie este folosită, probabil, în engleza britanică. John Bruce Lockhart, "Intelligence: A British View," în *Approaches to Intelligence*, ed. K.G.Robertson (Londra: Macmillan, 1978), 37, 46.
4. Această definiție a măsurilor active este preluată de la Richard H. Shultz și Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy* (McLean; Va: Pergamon-Brassey's, 1984), 193.
5. Statele Unite au inventat termenul "diplomație publică", care ar acoperi unele dintre tehnicile măsurilor active. Statele Unite nu au creat însă, structurile organizatorice care să permită aplicarea acestui concept. Directiva 77 a Deciziei de Securitate Națională (NSDD-77), din 14 ianuarie 1983, definește, în linii mari, diplomația publică, referindu-se la aceasta drept "acțiuni ale guvernului american menite să sprijine obiectivele noastre de securitate națională."
6. În lucrarea lor privind CIA, Victor Marchetti și John D. Marks s-au referit într-un mod critic la un program de antrenament pentru poliție, care se desfășura în sudul Vietnamului; oricum, cea mai mare nemulțumire a lor este legată de implicarea unei instituții academice, și anume Universitatea de stat Michigan, într-un program secret. Victor Marchetti și John D. Marks, *The CIA and the Cult of Intelligence* (New York: Knopf, 1974), 234.
7. Secțiunea 660 a Legii privind asistența externă din 1961, amendată în 1974 de L. 93-559 [22 USC 2420]. Această prevedere a fost modificată în 1985 prin adoptarea unei hotărâri privind scutirile acordate statelor Costa Rica, El Salvador și Honduras.

8. Un exemplu de controversă referitoare la schimbul de informaţii secrete şi dacă acestea ar trebui considerate activităţi secrete, s-a iscat în momentul în care Robert Gates a fost nominalizat pentru funcţia de Director al Agenţiei Centrale de Informaţii, în 1991. Această dispută se referea la decizia luată la începutul anului 1980 de către administraţia Reagan de a transmite anumite informaţii secrete Irakului, ca sprijin în războiul împotriva Iranului. Gates a argumentat că acţiunea s-a desfăşurat în condiţiile unei relaţii tradiţionale bazate pe schimbul de informaţii secrete. Oricum, senatorul Bill Bradley (D-N.J.) a sugerat faptul că, din moment ce acţiunea nu afecta schimbul reciproc de informaţii, ci influenţa operaţiunile militare ale Irakului, se încadra în categoria activităţilor secrete şi, în consecinţă, ar fi trebuit raportată Congresului. Consultaţi *Nomination of Robert Gates to Be Director of Central Intelligence: Hearings*, 102d Cong., prima sesiune, 1991, S. Hrg. 102-799 1, 578-79, 945-50, elaborată de Senatul Statelor Unite, Comisia specială privind activitatea serviciilor secrete.

9. Pentru o trecere în revistă a operaţiunilor sovietice de infiltrare în guvernul Statelor Unite din anii 1930 şi 1940, consultaţi John Earl Haynes şi Harvey Klehr, *Venona: Decoding Soviet Espionage in America* (New Haven, Connecticut: Yale University Press, 1999), capitolele 5-7, şi Herbert Romerstein şi Eric Breindel, *The Venona Secrets: Exposing Soviet Espionage and America's Traitors* (Washington, D.C.: Regnery, 2000).

10. Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev* (New York: HarperCollins, 1990; ediţia Harper-Perennial, 1991), 280-82, 334-37. În *The Venona Secrets*, 41-44, Romerstein şi Breindel susţin că White urma instrucţiunile sovietice în perioada anterioară atacului de la Pearl Harbor, atunci când a recomandat adoptarea unei politici dure faţă de Japonia. (Uniunea Sovietică considera, la vremea respectivă, tensiunile dintre Statele Unite şi Japonia drept o garanţie împotriva unui atac japonez asupra părţii de est a Uniunii Sovietice.) Conform surselor de ştiri citate de Haynes şi Klehr, Henry Wallace, vicepreşedinte în timpul administraţiei Roosevelt între anii 1941-1945, a remarcat că dacă ar fi câştigat alegerile, l-ar fi nominalizat pe White în funcţia de ministru al finanţelor şi pe Laurence Duggan, care a fost, de asemenea, agent sovietic, în funcţia de secretar de stat. Haynes and Klehr, *Venona*, 139 şi 411, nr. 49, şi Christopher Andrew şi Vasili Mitrohin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999), 105, 109.

11. Andrew şi Gordievsky, *KGB: The Inside Story*, 568-71.

12. Shultz şi Godson, *Dezinformatsia*, 133-49, cuprinde o discuţie a cazului şi o analiză detaliată a conţinutului buletinului informativ.

13. Shultz şi Godson, *Dezinformatsia*, 38. Andrew şi Gordievsky susţin că Harry Hopkins, unul dintre consilierii de încredere ai Preşedintelui Franklin Roosevelt, se numără printre agenţii de influenţă care l-au ajutat pe Roosevelt să-şi menţină statutul "neutru" în ceea ce-i priveşte pe principalii aliaţi ai Americii în război, Marea Britanie şi Uniunea Sovietică. Gordievsky pretinde că a asistat la o prezentare susţinută de cel care părea să-l controleze pe Hopkins în care era descris, în cel mai mic detaliu, rolul acestuia ca agent. Descrierea realizată de Gordievsky sugerează că Hopkins era manipulat, fără a-şi da seama, atât de Stalin, care îl linguşea ori de câte ori avea ocazia, cât şi de un ofiţer al serviciilor secrete sovietice, care pretindea a fi trimisul oficial al

liderului sovietic. Andrew şi Gordievsky, *KGB: The Inside Story*, 278, 334, 349-50. Pe de cealaltă parte, Romerstein şi Breindel (*The Venona Secrets*, 214-15) susţin că acele comunicaţii decriptate, interceptate de sovietici, care redau întâlnirile avute de Hopkins cu un *rezident* sovietic aflat în ilegalitate pe teritoriul Statelor Unite, indică faptul că Hopkins era, de fapt, un agent rus manipulat.

14. Materialul citat face parte din lucrarea lui Bob Woodward, "CIA Curried Favor with Khomeini, Exiles," *Washington Post*, 19 noiembrie 1986, A1, 28. Problema defectăriia fost relatată în "Soviet Diplomat in Iran Defects and Flees to Britain," *New York Times*, 24 octombrie 1982, A14.

15. Churchill relatează despre această tentativă în prezentarea celui de-al II-lea Război Mondial. Acesta a încercat să eludeze suspiciunile lui Stalin trimiţând un mesaj "concis şi criptic" care nu reprezenta o avertizare în ceea ce priveşte atacul german. Acest mesaj făcea, pur şi simplu, referire la mişcările trupelor germane care făceau aluzie la un astfel de atac. Churchill spera că un asemenea mesaj "va capta atenţia lui Stalin şi îl va face să cugete," ajungând, în final, singur la concluzia dorită. Din nefericire, aplicarea tacticii lui Churchill a fost, într-un fel, împiedicată de ambasadorul britanic la Moscova (*The Grand Alliance*, al treilea volum din seria *The Secret World War* [Boston: Houghton Mifflin, 1951], 357-61). Gabriel Gorodetsky, *Grand Delusion: Stalin and the German Invasion of Russia* (New Haven, Connecticut: Yale University Press, 1999), 155-78, susţine că povestea este mult mai complicată decât sugerează Churchill.

16. Richard H. Schultz Jr., *The Secret War against Hanoi: Kennedy's and Johnson's Use of Spies, Saboteurs, and Covert Warriors in North Vietnam* (New York: HarperCollins, 1999), 130-48, 162-63. Schultz aduce la cunoştinţă faptul că cei care administrează programul au realizat, în cele din urmă, că acesta nu subminează încrederea Vietnamului de Nord. În absenţa unei mişcări de rezistenţă reale, vietnamezii din regiunea de nord au ajuns, în timp, la ideea că alianţa era o farsă.

17. Ladislav Bittman, *The KGB and Soviet Disinformation: An Insider's View* (McLean, Virginia: Pergamon-Brassey's, 1985), 112-13.

18. Andrew şi Mitrokhin, *The Sword and the Shield*, 461-74.

19. Consultaţi lucrarea lui John Barron, *KGB Today: The Hidden Hand* (New York: Reader's Digest, 1983; New York: Berkley, 1985), 32-159, pentru relatarea lui Levchenko despre cariera sa în serviciile secrete urmată de dezertare.

20. Barron, *KGB Today,* 76-81, 85-90, şi 93-94. Articolul, sugerând că operaţiunile desfăşurate în calitate de dublu agent erau o provocare americană, urmărea reducerea sprijinului public pentru poziţia dură adoptată de guvernul japonez împotriva presiunii diplomatice sovietice. Agentul GRU a fost, de fapt, eliberat. Pe de altă parte, scrisoarea urmărea crearea unei presiuni publice asupra guvernului japonez pentru a da curs unei cereri venite din partea sovieticilor; prin aceasta se solicita ca pilotul să fie readus în ţară. Dar scrisoarea nu şi-a atins scopul.

21. Tăinuirea totală nu este întotdeauna posibilă. Astfel, un serviciu secret străin poate identifica locaţia de unde emite un post de radio "pirat" folosind echipament de detectare a direcţiei. În orice caz, această informaţie nu va fi disponibilă ascultătorului obişnuit.

22. G.J.A. O'Toole, *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action from the American Revolution to the CIA* (New York: Atlantic Monthly, 1991), 236-39. Articolele apărute în *Providence Journal* erau de obicei versiuni uşor exagerate ale informaţiei transmise de serviciile secrete. Efectul acestora era de a-i împiedica pe germani să afle că planul operaţiunilor lor fusese demascat. În mod similar, serviciile secrete britanice, acţionând clandestin, au făcut un efort imens pentru a determina întreaga Americă, înainte de intrarea acesteia în cel de-al doilea Război Mondial, să susţină Marea Britanie şi să respingă politica de izolare. Potrivit unor relatări secrete despre istoria Marii Britanii, printre acţiunile desfăşurate de serviciile secrete britanice în Statele Unite se numărau şi inventarea unor evenimente cu sprijinul anumitor jurnalişti prietenoşi, utilizarea unui post de radio din New York ca mijloc neavizat de propagandă, înfiinţarea de grupări paravan şi hărţuirea unor figuri marcante ale opoziţiei, care făceau parte din Congres şi din mişcarea muncitorească americană. Consultaţi David Ignatius, "How Churchill's Agents Secretly Manipulated the U.S. before Pearl Harbor," *Washington Post*, 17 septembrie 1989, secţiunea Outlook, 1. Rămâne încă neclară măsura în care programul britanic era secret faţă de guvernul american şi, în special, faţă de Preşedintele Roosevelt. Conform relatării lui Ignatius, în momentul în care istoria "secretă" a Marii Britanii a fost finalizată spre sfârşitul războiului, au fost împărţite copii ale acesteia atât lui Churchill cât şi oficialilor serviciilor secrete britanice, dar şi lui Roosevelt. Pentru o relatare a acestui eveniment, consultaţi Thomas E. Mahl, *Desperate Deception: British Covert Action Operations in the United States*, 1939-44 (Washington, D.C.: Brassey's, 1998). Printre acţiunile britanice mai erau incluse şi propaganda şi tot felul de "trucuri necinstite" al căror scop era înfrângerea lui Hamilton Fish, membru al Congresului şi susţinător al politicii de izolare (Capitolul 6).

23. Într-un studiu al CIA, "Soviet Covert Action and Propaganda" este analizat fenomenul Vocea Naţională a Iranului (NVOI), precum şi discursul acestuia, care îndeamnă la sentimente antiamericane. Acest studiu a fost prezentat de către directorul adjunct pentru operaţiuni al CIA, pe data de 6 februarie 1980 în faţa Subcomisiei de Supraveghere, Comisia Permanentă a Serviciilor Secrete, Camera Reprezentanţilor. Studiul este reprodus în lucrarea *Soviet Covert Action (The Forgery Offensive): Hearings*, a doua sesiune a Congresului al 96-lea, 1980, a Camerei Reprezentanţilor, Comisia Permanentă privind Activitatea Serviciilor Secrete, Subcomisia de Supraveghere. Prezentarea NVOI apare la paginile 78-79.

24. Ray S. Cline, *The CIA: Reality vs. Myth*, ediţie revizuită (Washington, D.C.: Acropolis, 1982), 151.

25. În urma confirmării publice de către senatorul Clifford Case a faptului că posturile de radio au beneficiat de fondurile acordate în secret de CIA, Congresul a decis în 1973 să sprijine, într-un mod deschis, operaţiunile radio prin intermediul Comitetului Internaţional de Radiodifuziune. Acest comitet a fost constituit ca agenţie federală independentă. Cord Meyer, *Facing Reality: From World Federalism to the CIA* (New York: Harper and Row, 1980), 110-13.

26. Discursul a fost, de asemenea, publicat în *New York Times*, care l-a primit de la Departamentul de Stat. Oricum, versiunea oferită mass-mediei străine includea 34 de paragrafe despre politica externă adoptată de sovietici, paragrafe care lipseau din versiunea din *New York Times*. Datorită faptului că Uniunea

Sovietică nu a contestat niciodată autenticitatea paragrafelor, John Ranelagh a concluzionat că acestea sunt veritabile (*The Agency: The Rise and Decline of the CIA* [New York: Simon şi Schuster, 1986], 287 n). Potrivit lui Ranelagh, CIA a primit două copii ale textului, o versiune completă (posibil de la o sursă din Uniunea Sovietică), precum şi o versiune corectată de la o sursă est-europeană. Explicaţia diferenţei dintre cele două versiuni ar fi protecţia sursei sovietice; versiunea completă a fost pusă numai la dispoziţia publicaţiilor non-americane, pentru a masca legătura cu serviciile secrete americane. Pare destul de plauzibilă şi varianta conform căreia cele 34 de paragrafe suplimentare puse la dispoziţia mass-mediei străine, au fost scrise de experţi CIA în stilul lui Hruşciov; scopul lor era acela de a crea o stare de confuzie în ţările blocului sovietic. Dacă este adevărat, motivul pentru care guvernul american a oferit publicaţiei *New York Times* numai versiunea autentică a discursului, a fost, probabil, acela de a se reduce posibilitatea ca opinia publică americană să fie indusă în eroare de către părţile fictive.

27. Jerrold L. Schecter şi Peter S. Deriabin, *The Spy Who Saved The World* (New York: Scribner, 1992), 380-88.

28. Ignatius, "How Churchill's Agents Secretly Manipulated the U.S. before Pearl Harbour." Consultaţi, de asemenea, Mahl, *Desperate Deception*, 34.

29. Pentru exemple şi discuţii referitoare la această tehnică şi la modul în care a fost utilizată de fosta Uniune Sovietică, consultaţi *Soviet Covert Action (The Forgery Offensive)*, Camera Reprezentanţilor, Comisia Permanentă privind Activitatea Serviciilor Secrete, şi *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-87*, august 1987, 29-32 şi 79-80, a Departamentului de Stat. A apărut o întrebare referitoare la o posibilă folosire a acestei tehnici de către S.U.A., făcându-se trimitere la faptul că CIA i-a adus la cunoştinţă lui Stalin conţinutul "discursului secret" a lui Hruşciov. Consultaţi nota nr. 26.

30. Termenul derivă din cuvântul rusesc *dezinformatsia*, care se referă la tehnica măsurilor active de a induce în eroare audienţa astfel încât aceasta să acţioneze în interesul vorbitorului. Consultaţi Shultz and Godson, *Dezinformatsia*, 194-95.

31. Edwin Meese III, *With Reagan: The Inside Story* (Washington, D.C.: Regnery Gateway, 1992), 170-71.

32. Susţinând, în faţa Curţii Constituţionale a Rusiei, scoaterea în afara legii în 1991 a Partidului Comunist, guvernul rus a pus la dispoziţia publicului o serie de documente din arhivele partidului, demonstrând că Departamentul de relaţii externe a sprijinit, în mod clandestin, de-a lungul anilor aproximativ 100 de partide şi grupări politice în 8 state. Până în 1988, 3 milioane de dolari au fost transferate în secret Partidului Comunist din Statele Unite; în anii 1980, peste 20 de milioane de dolari au fost transferate aceluiaşi partid. Aceste fonduri erau de obicei transmise beneficiarilor străini prin intermediul KGB. În anii 1920 şi 1930, organizaţia comunistă Comintern a fost folosită în acest scop. Consultaţi lucrarea lui Michael Dobbs, "Panhandling the Kremlin: How Gus Hall Got Millions," *Washington Post*, 1 martie 1992, A1, şi Harvey Klehr, John Earl Haynes, şi Kiril Mikhailovich Anderson, *The Soviet World of American Communism* (New Haven, Connecticut: Yale University Press, 1998), capitolul 2.

33. Pentru o scurtă prezentare a acestui efort, consultaţi Sallie Pisani, *The CIA and the Marshall Plan* (Lawrence: University Press of Kansas, 1991).

34. Cline, *The CIA*, 123-24.
35. Directiva Consiliului Național de Securitate 10/2 (Iunie 1948), citată în Cline, *The CIA*, 126.
36. Senatul Statelor Unite, Comisia Church, *Final Report*, volumul 1: *Foreign and Military Intelligence*, a doua sesiune a celui de-al 94-lea Congres, 1976, S. Rept. 94-755, 145.
37. Cline, *The CIA*, 150-51.
38. Comisia Church, *Staff Report: Covert Action in Chile: 1963-1973*, prima sesiune a celui de-al 94-lea Congres, 1975, Committee Print, 29, 45.
39. Comisia Church, *Staff Report*, 49 [ideea era subliniată în original].
40. Gregory F. Treverton, *Covert Action: The Limits of Intervention in the Postwar World* (New York: Basic Books, 1987), 142.
41. Treverton, *Covert Action*, 143.
42. La începutul Războiului Rece, CIA a organizat lovituri de stat în Iran (1953) şi Guatemala (1954). Kermit Roosevelt, *Countercoup: The Struggle for Control of Iran* (New York: McGraw-Hill, 1979); James Risen, "How a Plot Convulsed Iran in '53 (and in '79): A Secret CIA History," *New York Times*, 16 aprilie 2000; Nick Cullather, *Secret History: The CIA's Classified Account of Its Operations in Guatemala, 1952-54* (Stanford, California: Stanford University Press, 2000); şi Richard H. Immerman, *The CIA in Guatemala* (Austin: University of Texas Press, 1982).
43. Consultați lucrarea Comisiei Church, *Alleged Assassination Plots Involving Foreign Leaders: Interim Report*, prima sesiune a celui de-al 94-lea Congres, 1975, S. Rept. 94-465, pentru detalii referitoare la investigațiile realizate de comisie.
44. Ordinul executiv 11905, "United States Foreign Intelligence Activities," 18 februarie 1976, secțiunea 5(g) [41 Fed. Reg. 7733 (1976)].
45. Ordinul executiv 12036, 24 ianuarie 1978, secțiunea 2-305 [43 Fed. Reg. 3687 (1978)] şi Ordinul executiv 12333, 4 decembrie 1981, secțiunea 2.11 [48 Reg. Fed. 59947 (1981)]. Ambele prevederi renunță la adjectivul "politic," dar înțelesul este, probabil, același.
46. În linii mari, trebuie să se stabilească dacă ordinul executiv care interzice actele de asasinare interzice şi operațiunile care ar putea, din neatenție, să aibă ca rezultat moartea unui lider politic sau (mai restrictiv) expunerea unei personalități politice unui risc semnificativ de a fi ucis.
47. Jules Witcover, *Sabotage at Black Tom: Imperial Germany's Secret War in America, 1914-1917* (Chapel Hill, North Carolina: Algonquin, 1989).
48. Mărturia lui Stansfield Turner, în cadrul Camerei Reprezentanților, Comisia Permanentă privind Activitatea Serviciilor Secrete, Subcomisia pentru legislație, *HR 1013, HR 1371, and Other Proposals Which Address the Issue of Affording Prior Notice of Covert Actions to the Congress: Hearings*, prima sesiune a celui de-al 100-lea Congres, 1987, 44-49.
49. Pentru o relatare recentă privind programul de asistență acordată mujahedinilor de către o persoană implicată în conducerea unei rețele, consultați lucrarea lui Mohammad Yousaf şi Mark Adkin, *The Bear Trap: Afghanistan's Untold Story* (Londra: Leo Cooper, 1992). Yousaf a fost liderul departamentului pentru Afganistan al Serviciului secret pakistanez la mijlocul anilor 1980.

50. Sefton Delmer, *Black Boomerang* (New York: Viking, 1962), 120.

51. A se observa faptul că legea din anul 1991 (PL 102-88) care defineşte acţiunile secrete, se referă la activităţi "în care rolul guvernului Statelor Unite nu va fi evident sau nu va fi *recunoscut în mod public*" [subliniere adăugată]. Este vorba despre cazurile în care rolul guvernului, deşi evident pentru un observator al situaţiei internaţionale, sau chiar relatate în presă, nu este recunoscut în mod public.

52. Vezi discuţia referitoare la acest incident prezentată în capitolul 3.

53. Pentru o opinie favorabilă statutului acţiunilor secrete aflate sub incidenţa legislaţiei internaţionale, vezi lucrarea lui W. Michael Reisman şi James E. Baker, *Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law* (New Haven, Connecticut: Yale University Press, 1992). În general, Reisman şi Baker susţin că practica actuală a statelor, precum şi reacţia statelor şi a comunităţii internaţionale implică faptul că multe acţiuni secrete nu sunt neapărat ilegale din perspectiva legislaţiei internaţionale. Oricum, cei doi interpretează destul de strict principiul non-intervenţiei din Carta Naţiunilor Unite şi mult mai permisiv noţiuni cheie precum "activităţi secrete," "lege," şi "practica acceptată."

54. Nikita S. Hruşciov, *Hruşciov: The Last Testament* (Boston: Little, Brown, 1974), 447-48.

55. Vezi lucrarea lui John Dyson, *Sink the Rainbow! An Enquiry into the "Greenpeace Affair"* (Londra: Gollancz, 1986), 157-86, pentru o relatare a modului în care guvernului francez a gestionat acest episod.

56. Secţiunea 662(a) a Legii privind asistenţa externă din anul 1961, amendată. Amendamentul Hughes-Ryan a fost abrogat oficial odată cu punerea în aplicare a Legii privind autorizarea activităţii serviciilor secrete pentru anul fiscal 1991. Nouă lege păstra condiţia avizării de către preşedinte şi includea, de asemenea, cazul operaţiunilor secrete derulate nu numai de CIA, ci de toate agenţiile guvernamentale ale Statelor Unite. Legea dispunea ca toate hotărârile să fie "în scris". În cazul în care trebuie acţionat imediat, dar nu există timpul necesar pentru a emite o hotărâre scrisă, preşedintele este totuşi obligat să emită o astfel de hotărâre "în cel mult 48 de ore de la adoptarea deciziei" pentru autorizarea acţiunii.

57. Comisia Church a ignorat, în *Raportul Final*, chestiunea "negării plauzibile" în ceea ce priveşte efectele amendamentului. În schimb, în raport sunt prezentate cele două rezultate ale amendamentului, şi anume (1) responsabilitatea statutară a Executivului de a informa Congresul despre acţiunile secrete, şi (2) includerea comisiilor de politică externă ale Senatului şi Camerei Reprezentanţilor printre comisiile care trebuie informate. Volumul 1: *Foreign and Military Intelligence*, 151.

58. *Report of the Congressional Committees Investigating the Iran-Contra Affair*, prima sesiune a celui de-al 100-lea Congres, 1987, H. Rept. 100-433, S. Rept. 100-216, 271.

59. "Iraq Liberation Act of 1998," L. 105-338, 31 octombrie 1998. Măsura a fost adoptată ca urmare a rapoartelor referitoare la acţiunile secrete nereuşite ce aveau ca scop înlăturarea lui Saddam Hussein de la putere. Don Oberdorfer, "A Covert Plan to Oust Hussein," *Washington Post Weekly Edition*, 25-31 ianuarie 1993, 19, şi Jim Hoagland, "How CIA's Secret War on Saddam Collapsed,"

Washington Post, 26 iunie 1997, A21. Vezi, de asemenea, lucrarea lui Marie Colvin, "Revealed: CIA's Bungled Iraqi Coup," *The Sunday Times (London)*, 2 aprilie 2000.

60. David Lowe, în lucrarea "Idea to Reality: A Brief History of the National Endowment for Democracy," relatează despre istoria legislativă a înființării NED. Disponibil pe www.ned.org/about/about.html.

61. Spre exemplu, Fundația Konrad Adenauer (Stiftung) asociată cu Partidul Democrat Creştin, conform propriilor afirmații, au colaborat, mai mult de 30 de ani, cu parteneri din întreaga lume… Aceste acțiuni internaționale… sunt finanțate de Ministerul German Federal pentru Cooperare şi Dezvoltare Economică, Ministerul de Externe… Printre partenerii străini se numără partide politice, parlamente şi guverne; institute de educație şi cercetare; universități; confederații şi sindicate din industrie; cooperative; organizații feministe, de mediu şi de automotivare; şi mass-media. Toate aceste proiecte au ca scop promovarea democrației şi dezvoltarea, îmbunătățirea relațiilor interumane, indiferent de etnie, sprijinirea organizațiilor de automotivare şi combaterea cauzelor sărăciei şi distrugerii mediului. [citat pe www.kas.de/stiftung/englisch /international.html.]

62. Christopher Andrew, *Her Majesty's Secret Service: The Making of the British Intelligence Community* (New York: Viking, 1986), 476-77. S-a sugerat faptul că înființarea SOE ca agenție separată de MI6 s-a datorat, în parte, argumentelor politice interne. Plasând SOE în subordinea ministrului Economiei, membru al Partidului Laburist, Churchill răspuns solicitărilor partenerilor săi de coaliție, în sensul împărțirii controlului asupra serviciilor secrete. M. R. D. Foot, *SOE: An Outline History of the Special Operations Executive, 1940-46*, ediție revizuită (n.p.: University Publications of America, 1986), 19-20.

63. Comisia Church, *Final Report*, volumul 1, 106. Vezi, de asemenea, lucrarea lui Arthur B. Darling, *The Central Intelligence Agency: An Instrument of Government, to 1950* (University Park: Pennsylvania State University Press, 1990), 245-81. (Darling a fost istoric în cadrul CIA din 1952 până în 1954; inițial secretă, istoria lui Darling a fost publicată în 1989, în colaborare cu Departamentul de cercetare istorică al Agenției.)

64. Mai târziu, denumirea a fost schimbată în Direcția de Operațiuni (DDO).

65. Comisia Church, *Final Report*, volumul 1, 107-108.

66. Pentru o opinie critică referitoare la componentele activității de informații, consultați lucrarea lui Kenneth G. Robertson, "The Study of Intelligence in the United States," apărută în *Comparing Foreign Intelligence: The U.S., the USSR, the UK and the Third World*, editor Roy Godson (McLean, Virginia: Pergamon-Brassey's, 1988), 26-28.

67. George Kennan, oficial al Departamentului de Stat, care a contribuit la stabilirea normelor operaționale inițiale ale OPC, a afirmat că acțiunile secrete au fost un instrument folosit în politica externă. În consecință, aceste acțiuni secrete intrau exclusiv în responsabilitatea Departamentului de Stat şi a instituțiilor militare naționale. Datorită anumitor caracteristici, OPC putea fi considerată parte a Agenției Centrale de Informații, dar strategia şi orientarea erau impuse de către Departamentul de Stat şi organele puterii de stat. Astfel, pe timp de pace, secretarul de stat era cel care îl numea pe liderul OPC şi îi supraveghea activitățile. Darling, *The Central Intelligence Agency*, 277.

CAPITOLUL 5: SPION CONTRA SPION: CONTRAINFORMAȚIILE

1. Termenul *contraspionaj* poate fi definit ca fiind o formă de protecție împotriva "sabotajului sau asasinatelor comise de către sau în numele unor puteri, organizații sau persoane străine, sau împotriva activităților de terorism internațional." (Citatul face parte din definiția contraspionajului prezentată în Ordinul executiv 12333 al președintelui Reagan din 4 decembrie 1981, "United States Intelligence Activities," paragraful 3.4[a].) Aceasta poate fi considerată o definiție potrivită, din moment ce aceste acțiuni sunt identice sau similare cu acțiunile secrete desfăşurate de un serviciu secret al unui stat inamic; protecția împotriva acestora poate implica, aşadar, multe dintre metodele folosite împotriva acțiunilor serviciilor secrete ale statelor dușmane.
2. Definiția contraspionajului din ordinul executiv la care ne-am referit în cadrul notei 1 exclude "programele de securitate a comunicațiilor, documentelor şi personalului." Astfel, este reflectat faptul că, în general, ministerele şi agențiile americane care lucrează cu informații secrete sunt responsabile pentru programele de securitate, pentru a proteja acele informații, în timp ce principala responsabilitate a FBI-ului şi CIA-ului se referă la acțiunile de contraspionaj (ținând cont de definiția din ordinul executiv), desfăşurate atât în țară, cât şi în străinătate. Oricum, din punctul nostru de vedere, securitatea ar trebui considerată ca fiind parte a contraspionajului, din moment ce ambele îndeplinesc aceeaşi funcție.
3. Harold C. Relyea, "The Presidency and the People's Right to Know," în *The Presidency and Information Policy*, editat de Harold C. Relyea (New York: Center for the Study of the Presidency, 1981), 11-19.
4. "Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Departments and Agencies of the Executive Branch, of Official Information Which Requires Safeguarding in the Interest of the Security of the United States," Ordinul Executiv 10290, 24 septembrie 1951.
5. Ordinul Executiv 12958, "Classified National Security Information," 17 aprilie 1995. Biroul pentru supravegherea securității informațiilor (ISOO) este responsabil cu supravegherea programului guvernamental de securitate a informațiilor clasificate. Raportul anual al ISSO oferă o scurtă trecere în revistă a programului de clasificare şi declasificare a informațiilor. Potrivit celui mai recent raport, 3846 de oficiali guvernamentali au deținut dreptul de clasificare a informațiilor; în decursul anului, s-au luat mai mult de opt milioane de decizii de clasificare a documentelor. Dintre acestea, 44% aparțin CIA-ului; 27%, Ministerului Apărării; Biroului Național de Recunoaştere, 24%; Ministerului Justiției, 2%, Departamentului de Stat, 2%; şi celorlalte agenții, 1%. (Aproape 127 de milioane de pagini ale unor materiale clasificate în trecut au fost declasificate.) ISOO, *FY1999 Report to the President*, 15 august 2000. Rapoartele anuale ale ISOO sunt disponibile la adresa www.fas.org/sgp/isoo/index.html.
6. Ordinul Executiv 12958, secțiunea 1.3.
7. Legea Securității Naționale emisă în anul 1947, secțiunea 102(d) (3) [50 USC 403 (d) (3)]. Ordinul Executiv 12958, secțiunea 4.4, îi autorizează pe Directorul Agenției Centrale de Informații, precum şi pe miniştrii de Externe, ai Apărării şi ai Industriei energetice să creeze programe speciale de acces.

8. Ordinul Executiv 12958, secţiunea 4.4(a) şi (b)(3). Echipa de supraveghere este condusă de directorul Biroului pentru supravegherea securităţii informaţiilor, care este responsabil pentru sistemul de clasificare a informaţiilor referitoare la siguranţa naţională.

9. Ordinul Executiv 12958 defineşte "nevoia de a şti" drept "stabilirea de către deţinătorul de informaţii clasificate a faptului că un potenţial beneficiar are nevoie de acces… pentru a-şi îndeplini, în mod legal şi autorizat, toate atribuţiile funcţiei sale guvernamentale" (secţiunea 4.1[c]).

10. *Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices*, 23 noiembrie 1985, citat în *Meeting the Espionage Challenge: A review of United States Counterintelligence and Security Programs*, a doua sesiune a celui de-al 99-lea Congres, 1986, S. Rept. 99-522, 66, aparţinând Statului American, Comisia Specială pentru Serviciile Secrete.

11. Până în 1989, Uniunea Sovietică a dat publicităţii o singură cifră, despre care a spus că reprezintă bugetul pentru apărare. Totuşi, cifra era, în mod evident, mult prea mică pentru a include toate cheltuielile militare sovietice. În 1989, când au făcut publică o valoare totală mult mai mare a cheltuielilor pentru apărare, sovieticilor au explicat că cifra publicată anterior includea numai salariile şi normele de întreţinere ale membrilor forţelor armate. În mod similar, Republica Populară Chineză a publicat o cifră despre care pretindea că reprezintă cheltuielile pentru apărare; şi această cifră era, de asemenea, mult prea mică, dar nu se ştie ce componentă a cheltuielilor de apărare includea, de fapt, dacă cifra reprezenta, într-adevăr, ceva.

12. *Keeping the Nation's Secrets*, 49.

13. Pentru o analiză mai detaliată a sistemului păstrării secretului oficial în Marea Britanie, care este comparat, în linii mari, cu cel din Suedia şi Statele Unite, consultaţi lucrarea lui K. G. Robertson, *Public Secrets: A Study in the Development of Government Secrecy* (New York: St. Martin's, 1982). De la publicarea studiului lui Robertson, Marea Britanie a adoptat două legi referitoare la păstrarea secretului guvernamental: un amendament (în 1989) la Legea Secretelor Oficiale, şi o Lege a Dreptului la Liberă Informare (în 2000.) Pentru o analiză a Legii Secretelor Oficiale şi a amendamentului din 1989, consultaţi lucrarea lui Rosamund Thomas, *Espionage and Secrecy: The Official Secrets Acts 1911-1989 of the United Kingdom* (New York: Routledge, 1991). Textul Legii Dreptului la Liberă Informare este disponibil la adresa www.legislation.hmso.gov.uk/ acts/acts2000/20000036.htm.

14. În 1997, o comisie înfiinţată pentru a analiza programele guvernamentale de clasificare a informaţiilor secrete a susţinut faptul că "sistemul de clasificare … este folosit prea des pentru a nega dreptul populaţiei de a înţelege procesul de luare a deciziilor politice" şi că "cea mai bună metodă de a fi siguri de păstrarea secretelor, mai ales a secretelor importante care trebuie *să rămână* secrete, este ca secretizarea să revină la rolul său limitat, dar necesar. Secretele pot fi păstrate într-un mod mult mai eficient, dacă se renunţă la tăinuirea lor." *Secrecy: Report of the Commission on Protecting and Reducing Government Secrecy* (Washington, D.C.: Government Printing Office, 1997), xxi [în original, ideea este accentuată], este disponibil la adresa www.access.gpo.gov/int.

15. Ordinul Executiv 12958 menționează faptul că "informațiile secrete nu vor fi, în niciun caz, clasificate doar pentru ca o persoană, organizație sau agenție să nu fie puse într-o lumină proastă" (secțiunea 1.8[a][2]). Există totuși posibilitatea ca informațiile să fie în continuare clasificate pentru ca guvernul să nu fie pus într-o lumină proastă. Acest lucru este subliniat de faptul că "informațiile care ar putea afecta relațiile dintre Statele Unite și un guvern străin" nu sunt declasificate în mod automat (secțiunea 3.4[b][6]).

16. Bob Woodward, "CIA Paid Millions to Jordan's King Hussein," *Washington Post*, 18 februarie 1977, A1.

17. Legea energiei atomice din anul 1954, secțiunea 11y [42 USC 2014y].

18. Secțiunea 148 [42 USC 2168].

19. Adm. B. R. Inman, "National Security and Technical Information," lucrare prezentată în cadrul întrunirii anuale a Societății americane pentru progresul științei, ianuarie 1982, Washington, D.C.

20. Senatul Statelor Unite ale Americii, Comisia pentru Comerț, Știință și Transporturi, *Statement of Louis J. Freeh, Director, FBI, on July 25 1996, Regarding "Impact of Encryption on Law Enforcement and Public Safety"*. Disponibil la adresa www.fas.org./irp/congress/1996_hr/s960725f.htm.

21. S-a sugerat ca toți producătorii de programe de criptare să asigure un "escrow key" – adică informațiile care să permită o decriptare cât mai rapidă. Astfel, o agenție de aplicare a legii ar putea folosi această cheie pentru a citi materialele interceptate sau informațiile dintr-un calculator, toate acestea realizându-se pe baza unui mandat de percheziție. Potrivit lui Freeh, directorul FBI, tipurile speciale de criptare disponibile pe piață "pot afecta echilibrul legal și așa delicat asigurat prin cel de-al Patrulea Amendament al Constituției S.U.A., din moment ce, atunci când un judecător emite un mandat de percheziție, mandatul nu va avea nicio valoare practică în cazul unei astfel de criptări" (declarația lui Freeh). Potrivit lui Freeh, criptarea ce utilizează "escrow key" ar putea contribui la restabilirea echilibrului legal, însă acest argument nu s-a bucurat de sprijin.

22. Pe 12 ianuarie 2000, Ministerul Comerțului din Statele Unite a emis o serie de norme care permiteau, în mare măsură, exportul neîngrădit al unor programe de criptare foarte avansate. Declarația de presă a Ministerului Comerțului este disponibilă la adresa www.fas.org/irp/news/2000/01/000113-crypto-bxa.htm.

23. În Statele Unite, cel puțin la nivel teoretic, lipsa de loialitate față de guvern nu permite niciunei persoane deținerea unei funcții în serviciile publice federale; totuși, s-a renunțat la acest criteriu în cazul posturilor care nu solicită acces la informațiile clasificate. Consultați lucrarea lui Guenter Lewy, "The Federal Loyalty-Security Program," în *Intelligence Requirements for the 1980's: Domestic Intelligence*, editată de Roy Godson (Lexington, Massachusetts: Lexington, 1986), 147 și passim, pentru o analiză a acestei evoluții. Aspectul loialității este prezentat în Ordinul Executiv 10450 al președintelui Truman, "Security Requirements for Government Employment," 27 aprilie 1953.

24. Cu condiția ca această convingere nu a stat la baza niciunei acțiuni violente sau criminale. Chiar și în acest caz, nu ar fi fost admisibilă întocmirea unei liste complete cu membrii organizației, cu excepția cazului în care nu se putea demonstra că membrii acesteia, în general, erau implicați în acțiunile violente ale organizației. Aceste aspecte sunt analizate în capitolul următor.

25. Senatul Statelor Unite ale Americii, Subcomisia pentru legi şi proceduri penale, Comisia pentru Justiţie, *Hearings on the Erosion of Law Enforcement Intelligence and Its Impact on the Public Security*, partea a opta, a doua sesiune al celui de-al 95-lea Congres, 1978, citat în lucrarea lui Guenter Lewy, "The Federal Loyalty-Security Program," 152.

26. În 1983, Biroul de Evaluare a Tehnologiei (OTA) al Congresului Statelor Unite a elaborat un studiu critic la adresa reclamaţiilor întemeiate pe rezultatele testului poligraf. *Scientific Validity of Polygraph Testing: A Research Review and Evaluation-Technical Memorandum*, OTA-TM-H-15 (Washington, D.C.: Government Printing Office, 1983). Anul următor, Ministerul Apărării, a cărui Agenţie Naţională de Securitate foloseşte poligraful, a publicat un studiu care îl combătea pe cel dintâi. Ministerul Apărării Statelor Unite, *The Accuracy and Utility of Polygraph Testing* (Washington, D.C.: Government Printing Office, 1984).

27. Vezi analiza din cadrul acestui capitol a operaţiunii cubaneze de inducere în eroare, derulată împotriva Statelor Unite. Cel puţin doi dintre aceşti agenţi dubli, pe care comunitatea serviciilor secrete îi considera loiali, au fost supuşi unor teste cu poligraful.

28. Aceste teste poligraf sunt analizate în Senatul Statelor Unite, Comisia specială pentru activitatea serviciilor secrete, *An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence*, 1 noiembrie 1994, 32-34, 71-74. Potrivit FBI, analiza din iunie 1993 a rezultatelor testelor poligrafice realizate în 1986 de către experţii instituţiei a demonstrat faptul că Ames minţise; oricum, până la momentul efectuării acestei reexaminări, Ames făcea deja obiectul unor "anchete serioase" (82). Este, aşadar, dificil de ştiut în ce măsură următoarea analiză a rezultatelor testelor poligraf a fost afectată de faptul că existau multe suspiciuni.

29. Vezi *Meeting the Espionage Challenge*, 12-15, Senatul Statelor Unite, Comisia specială pentru activitatea serviciilor secrete, pentru o trecere în revistă a cazurilor dintre 1980-1986. Pentru o listă a cazuri de după această perioadă, vezi lucrarea Serviciului de Securitate al Ministerului Apărării, *Recent Espionage Cases, 1975-1999: Summaries and Sources,* Security Research Center (septembrie 1999), disponibilă pe www.dss.mil/training/pub.htm.

30. Spre exemplu, un subofiţer din cadrul armatei care a vândut informaţii strict secrete obţinute din interceptarea comunicaţiilor, Uniunii Sovietice şi statelor semnatare ale Pactului de la Varşovia, vreme de şase ani, i-a spus unui agent sub acoperire al FBI următoarele: "nu aveam probleme cu banii. Am hotărât doar că nu mai vreau ca niciodată să mă gândesc de unde voi face rost de următorul dolar. Nu sunt împotriva Americii. Preţuiesc steagul la fel de mult ca oricare altă persoană." Serviciul de Securitate al Ministerului Apărării, *Recent Espionage Cases*, 22.

31. Pe de altă parte, se pare că Hanssen nu fusese motivat nici de lăcomie. El susţine, într-un mesaj, că a început să admire serviciile secrete sovietice la vârsta de 14 ani, în momentul în care a citit memoriile lui Kim Philby; este total lipsit de sens, din moment ce Hanssen s-a născut în 1944, iar cartea lui Philby a fost publicată abia în anul 1960. Acest mesaj este citat în depoziţia guvernului Statelor Unite ale Americii în favoarea arestării şi emiterii de mandate de percheziţie împotriva lui Hanssen, depusă la dosar la US District

Court din Virginia de Est. (Potrivit altor mesaje citate în depoziție, Hanssen nu pare a fi foarte îngrijorat când e vorba de bani, deşi acesta solicită o sumă inițială de o sută de mii de dolari.) Depoziția este disponibilă la adresa www.fas.org/irp/ops/ci/hanssen_affidavit.html.

32. După cum se menționează într-un raport al Comisiei Senatoriale pentru activitatea serviciilor secrete, "amenințarea venită din partea altor servicii secrete ostile la adresa sistemelor informaționale americane este amplificată de creşterea surprinzătoare a numărului şi performanțelor computerelor, precum şi a volumului de informații stocate în acestea… Computerele sporesc foarte mult numărul informațiilor la care poate avea acces o persoană." (*Meeting the Espionage Challenge*, 35-36.) Pentru o relatare documentată a problemelor specifice sistemelor computerizate de securitate, precum şi a cazurilor de spionaj în domeniu, vezi lucrarea lui Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989).

33. Pentru un exemplu, consultați nota 70 a capitolului 2.

34. Senatul Statelor Unite ale Americii, Comisia specială privind activitatea serviciilor secrete, *Meeting the Espionage Challenge*, 34-35.

35. După cum afirma în anul 1987 James Schlesinger, fost ministru al Apărării,

    În ultimii ani, sovieticii ne urmăreau îndeaproape, astfel încât am putut detecta şi înlătura infiltrările… În momentul de față, ne confruntăm cu un progres al tehnologiei sovietice, care, totuşi, nu este mai avansată decât tehnologia noastră; într-adevăr, în anumite domenii au fost cu un pas înaintea noastră… Avem multe de învățat de la sovietici, atât în ceea ce priveşte construcția de ambasade, cât şi cu privire la derularea de operațiuni. Sovieticii s-au gândit îndelung la crearea unor sisteme de securitate speciale pentru ambasade, precum şi la construcția acestora.

    Mărturia lui James Schlesinger în fața Comisiei Senatoriale pentru Buget, conform citatului din articolul "For the Record," *Washington Post*, 1 iulie 1987, A18.

36. Christopher Andrew şi Oleg Gordievsky, *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev* (New York: Harper Collins, 1990; ediția Harper-Perennial, 1991), 296-98, şi 598-99.

37. După cum am menționat deja, Howard a reuşit să se sustragă supravegherii FBI şi, câteva luni mai târziu, a fost văzut la Moscova. Yurchenko a revenit în Uniunea Sovietică, fapt ce sugerează că este posibil ca actul său inițial de trădare să fi fost o înscenare, iar el să fi fost trimis de sovietici pentru a induce în eroare serviciile secrete americane, sau pentru un alt motiv. Dacă aceasta este situația, pentru a întări autenticitatea faptelor lui Yurchenko sau buna sa credință s-a renunțat la Pelton şi la Howard - care nu mai erau angajați de SUA sau nu mai erau de niciun folos sovieticilor. Vezi David Wise, *The Spy Who Got Away: The Inside Story of Edward Lee Howard* (New York: Random House, 1988), 17-21 şi passim.

38. Pentru o discuție despre "Tricycle" (tricicletă) (un iugoslav pe nume Dusko Popov) şi despre modul de utilizare al chestionarului, vezi B. Bruce Briggs, "Another Ride on Tricycle", *Intelligence and National Security* 7, nr.2 (aprilie 1992): 77-100. Este de remarcat faptul că, acest chestionar a ajuns în mâinile

americanilor odată cu mesajul japonez despre un "atac cu bombă" din septembrie 1941. În acest mesaj interceptat se solicita consulatului japonez din Honolulu să indice cu exactitate care sunt cabinele navelor americane de la Pearl Harbour. Mesajul a fost decodificat, dar se pare că nimeni nu s-a întrebat de ce aveau japonezii nevoie de informaţii atât de detaliate. Vezi Gordon W. Prange, *At Dawn We Slept: The Untold Story of Pearl Harbour* (New York: McGraw-Hill, 1981), 248-52.

39. Pentru detalii despre agentul american dublu cu activitatea cea mai îndelungată din timpul Războiului Rece, vezi David Wise, *Cassidy's Run: The Secret Spy War Over Nerve Gas* (New York: Random House, 2000), povestea unui sergent major din armata americană, Joseph Cassidy, care a fost "fluturat" prin faţa serviciilor secrete sovietice şi care a lucrat ca agent dublu peste 20 ani. Potrivit lui Wise, în urma acestei activităţi au fost demascaţi aproape doisprezece ofiţeri ruşi, au apărut trei "emigranţi ilegali" şi un "cod Armaghedon" utilizat de serviciile secrete ruse. În această perioadă, Cassidy a furnizat peste 4500 de pagini de documente clasificate ruşilor, inclusiv "informaţii" menite să îi inducă în eroare pe sovietici cu privire la succesul înregistrat de americani în încercările lor de obţinere a armelor chimice. Unul dintre scopurile americanilor a fost să îi determine pe ruşi să cheltuiască timp şi resurse pe o formulă despre care oamenii de ştiinţă americani stabiliseră deja că nu este eficientă (63-69). Wise bănuieşte că înşelăciunea s-a întors împotriva lor atunci când sovieticii au reuşit să depăşească obstacolele care îi blocaseră pe americani şi au produs o nouă substanţă chimică letală; cu toate acestea, dovezile în favoarea acestei opinii sunt circumstanţiale şi nici foarte convingătoare (63-69).

40. John C. Masterman, *The Double-Cross System in the War of 1939 to 1945* (New Haven, Connecticut: Yale University Press, 1972), 3. Această lucrare, elaborată de cel care a condus sistemul este sursa relatării din text; pentru mai multe detalii vezi pag. 30-31, 38-40, 41, 49 şi 58.

41. Agentul care lucrase iniţial pentru serviciul militar de informaţii german (Abwehr) la sfârşitul anilor 1930; britanicii care ştiau de existenţa lui i-au permis să îşi continue activitatea în parte şi pentru că acesta colabora cu MI6, ceea ce ar fi complicat eforturile de a-l urmări în justiţie.

42. Chiar şi după ce aliaţii au acostat în Normandia în data de 6 iunie, agenţii dubli britanici şi-au continuat activitatea. De exemplu, pe data de 9 iunie, "Garbo" (nume de cod pentru Juan Pujol, unul dintre cei mai de succes agenţi dubli ai MI5) a difuzat prin radio la Berlin ştirea că invazia din Normandia era o diversiune menită să atragă rezervele germane şi să slăbească forţele care protejau Calais-ul, unde avea să aibă loc adevăratul atac. La primirea acestui mesaj, înaltul comandament german a contramandat ordinul dat anterior privind un contraatac german asupra forţelor aliate pe plaja din Normandia. Drept mulţumire pentru "informaţia" furnizată de Pujol, Hitler i-a conferit Crucea de Fier. Christopher Andrew, *Her Majesty's Secret Service: The Making of the British Intelligence Community* (New York:Viking, 1986), 488. Pentru informaţii privind viaţa lui Pujol ca dublu agent britanic, vezi Juan Pujol şi Nigel West, *Garbo* (Londra:Weidenfeld şi Nicolson, 1985).

43. Michael Wines şi Ronald J.Ostrow, "Cuban Defector Claims Double Agents Duped U.S.," *Washington Post*, 12 august, 1987, A8.

44. Potrivit unui important membru al minorităților din Comisia permanentă privind activitatea serviciilor de informații, din Camera Reprezentanților, s-a descoperit că "aproape toți" "agenții est germani" recrutați de americani erau "agenți dubli". Bud Shuster, "HiTech vs. Human Spying," *Washington Times*, 11 februarie 1992, F3.

45. Directorul NSA, gen. lt. Michael V. Hayden, USAF a descris în felul următor principalele provocări pe care le-a înfruntat agenția sa: "Mijloacele de comunicații ale adversarului nostru sunt influențate de ciclul de dezvoltare al industriei globale care se mișcă cu viteza luminii [-]…telefoane celulare, mijloace de criptare, *comunicații prin intermediul fibrei optice*, comunicații digitale." Dan Verton, "NSA Warns It Can't Keep Up with Rapid Changes in IT," Infoworld.com, 19 februarie 2001 [subliniere în text].

46. Pentru două discuții generale despre problema tacticii militare de dezinformare vezi *Strategic Military Deception* editată de Donald Daniel şi Katherine Herbig, (New York: Pergamon, 1982) şi John Gooch şi Amos Perlmutter, *Military Deception and Strategic Surprise* (Londra: Frank Cass, 1982).

47. Despre tacticile de dezinformare folosite înainte şi în timpul celui de-al Doilea Război Mondial, vezi: Michael Howard, *British Intelligence in the Second World War: Strategic Deception* (Londra: Her Majesty's Stationery Office, 1990); Michael Mihalka, *German Strategic Deception in the 1930's*, RandNote N-1557-NA (Santa Monica, California: RAND, 1980); Barton Whaley, "Covert Rearmament in Germany 1919-1939: Deception and Misperception," *Journal of Strategic Studies*, nr.5 (martie 1982): 3-39; Barton Whaley, *Codeword Barbarossa* (Cambridge, Massachussets: MIT, 1973); David M. Glantz, *Soviet Military Deception in the Second World War* (Londra: Frank Cass, 1989); Charles Cruickshank, *Deception in World War II* (Oxford: Oxford University Press, 1979); *Strategic and Operational Deception in the Second World War* editată de Michael Handel (Londra: Frank Cass, 1987); şi o ediție specială a *Intelligence and National Security* 2, nr.3 (iulie 1987).

48. "Cheka" este un acronim bazat pe cel de-al doilea şi cel de-al treilea cuvânt din denumirea în limba rusă a "All – Russian Extraordinary Commission to Combat Counterrevolution and Sabotage." (Comisia rusă extraordinară de combatere a contrarevoluției şi a sabotajului)

49. Pentru o discuție despre Trust, vezi John J. Dziak, *Chekisty: A History of the KGB* (Lexington, Massachussets: Heath, Lexington, 1988), 47-50 şi Andrew şi Gordievsky, *KGB: The Inside Story*, 97-106.

    În mod similar, serviciile de informații sovietice şi cele poloneze după al Doilea Război Mondial utilizând un agent polonez dublu au reuşit să îi convingă pe britanici şi pe americani că un grup de rezistență polonez (Wolnosc i Niepodleglosc, WiN) era încă activ şi necesita asistență secretă; de fapt, WiN era controlat de KGB şi de serviciile de informații poloneze. Până în 1952, când polonezii şi sovieticii au recunoscut activitatea de dezinformare, serviciul secret polonez s-a folosit de WiN pentru a descoperi ultimii membri activi ai rezistenței anticomuniste din Polonia şi pentru a transmite informații eronate despre situația internă din Polonia în Occident. Dziak, *Chekisty*, 123-24.

50. John Prados, *The Soviet Estimate: U.S. Intelligence analysis and Russian Military Strength* (New York: Dial, 1982), 42-43.

51. Vezi Arnold L. Horelic şi Myron Rush, *Strategic Power and Soviet Foreign Policy* (Chicago: University of Chicago Press, 1966), 42-116, pentru o discuție pe larg despre aceste declarații exagerate şi scopul lor.

52. Horelick şi Rush, *Strategic Power*, 117- 40.

53. Prange, *At Dawn We Slept*, 338, 353.

54. Trebuie să ținem, de asemenea, cont de modul în care adversarul procesează informațiile. Dacă, de exemplu, din cauza timpului scurt avut la dispoziție, nu va fi timp să analizeze pe îndelete fotografiile înainte de a lua o decizie atunci poate fi indus în eroare printr-o imitație de calitate inferioară. Până când o analiză detaliată îi va fi indicat adversarului faptul că obiectivul este unul fals, acesta va fi acționat deja pe baza primei impresii greşite. Iată un alt motiv pentru care operațiunile de dezinformare sunt utilizate mai des în timp de război decât în timp de pace.

55. Howard, *British Intelligence in the Second World War: Strategic Deception*, 224.

56. H.J. Giskes, *London Calling North Pole* (Londra: William Kimber, 1953) şi M. R. D. Foot, *SOE: An Outline History of the Special Operations Executive*, *1940 - 46*, ediție revăzută (Frederick, Dr.: University Publications of America, 1986), 130-34. Giskes era ofițerul german de contrainformații care conducea operațiunea. Se pare că germanii nu au folosit acest canal pentru a-i induce în eroare pe britanici privind alte activități decât cele ale agenților lor SOE din Olanda.

57. Acest incident este relatat în cartea lui H. M. G. Lauwers, "Epilogue", în Giskes, *London Calling North Pole*, 194. Lauwers un agent SOE olandez capturat de germani, a încercat fără succes să informeze Londra cu privire la operațiunea de dezinformare prin transmiterea de mesaje fără a-şi lua însă măsurile de siguranță necesare. Din nefericire, comandamentul a ignorat acest aspect şi a considerat mesajele ca fiind autentice.

    Leo Marks, ofițerul responsabil cu codurile SOE, sugerează că suspciunile privind agenții din Olanda au fost atenuate de temerea conducerii SOE că, dacă se confirma un eşec de o asemenea anvergură, organizația ar fi fost închisă sau subordonată rivalului său din punct de vedere birocratic, Serviciului de informații externe, MI6. *Between Silk and Cyanide: The Story of the S.O.E.'s Code War* (Londra: HarperCollins, 1998), 112-25, 146-48.

58. Stansfield Turner, *Secrecy and Democracy: The CIA in Transition* (Boston: Houghton Mifflin, 1985; Harper and Row, 1986), 65.

59. Ca şi în alte cazuri, aici este necesar să se ajungă la un compromis. O variație pe orbită înseamnă că anumiți sateliți urmează orbite care nu au acoperire optimă; este necesar un echilibru între măsurile obişnuite de eficientizare a costurilor şi măsura mai subtilă de contracarare a operațiunilor de acoperire şi de dezinformare ale adversarului.

60. David Kahn, expert în criptare, susține acest punct de vedere în "Discussion," în *Intelligence Requirements for the 1980s: Clandestine Collection*, editată de Roy Godson (Washington, D.C.: National Strategy Information Center, 1982), 119.

61. Andrew şi Gordievsky, *KGB: The Inside Story*, 529-30, 610.

62. Procesele verbale ale şedinţelor de planificare sunt reproduse în David E. Murphy, Serghei A. Kondrashev şi George Bailey, *Battleground Berlin: CIA vs. KGB in the Cold War* (New Haven, Connecticut: Yale University Press, 1997), 449-53.

63. CIA a observat că un echipament electric de cifrare transmitea un semnal electric reprezentând un caracter obişnuit împreună cu caracterul cifrat; semnalul iniţial, deşi slab în comparaţie cu cel cifrat, putea fi receptat pe firul de transmisie, la o distanţă apreciabilă de echipamentul de cifrare. S-a descoperit că echipamentele sovietice de cifrare prezentau acelaşi dezavantaj, ceea ce le-a permis SUA să recupereze mesajele cu caractere obişnuite cât şi versiunile lor criptate. John Ranelagh. *The Agency: The Rise and Decline of the CIA* (New York: Simon and Schuster, 1986), 140.

    Murphy şi alţii, *Battleground Berlin*, neagă existenţa acestui "efect de ecou" (206-207). Este imposibil să lămurim acest aspect în lucrarea de faţă; relatarea din text are menirea de a ilustra tipul de implicaţii la care poate da naştere acest gen de operaţiuni.

64. Murphy şi alţii, *Battleground Berlin*, 289.

65. Murphy şi alţii, *Battleground Berlin*, 295.

66. De ce ar fi dorit sovieticii să încheie operaţiunea dacă avea drept scop transmiterea de informaţii false? Ar fi putut face acest lucru pentru a dăuna moralului angajaţilor CIA şi MI6 considerând că puterile occidentale aveau să descopere oricum cât de curând adevărul despre această operaţiune. Sau, sovieticii au oprit operaţiunea pur şi simplu deoarece costurile implicate de furnizarea de "material de dezinformare" (informaţii autentice oferite în mod voit inamicului pentru a întări credibilitatea operaţiunii) erau mai mari decât puteau ei să plătească. Este posibil ca descoperirea să fi fost făcută accidental, în sensul că echipa de intervenţie nu avea cunoştinţă de acest tunel peste care a dat, deoarece aceia care ştiau nu luaseră măsurile necesare pentru interzicerea lucrărilor în zona tunelului (dacă sovieticii desfăşurau o operaţiune de dezinformare numai un cerc restrâns de oameni avea cunoştinţă de acest lucru). Dacă SUA şi Marea Britanie ar fi aflat despre această descoperire, ar fi devenit suspicioşi în momentul în care ruşii ar fi continuat să folosească în continuare cablul fără a îndepărta mijloacele de interceptare.

67. Cruickshank, *Deception in World War II*, 182.

68. Întreaga controversă a fost denumită "pustiul oglinzilor" şi este subiectul unei cărţi cu acelaşi titlu de David Martin (New York: Harper and Row, 1980). Pentru mai multe lucrări recente pe marginea acestei controverse, vezi David Wise, *Molehunt: The Secret Search fot the Traitors that Shattered the CIA* (New York: Random House, 1992) şi lucrările citate în nota 35, capitolul 2.

69. John Barron, *Breaking the Ring* (Boston: Houghton Mifflin, 1987), 23-25.

70. Discuţia are ca sursă lucrările Comisiei senatoriale privind activitatea serviciilor de informaţii, *An Assessment of the Aldrich H. Ames Espionage Case*, 24-28.

71. În mod ironic, decizia KGB de a închide toate cazurile în acelaşi timp indică faptul că KGB *nu* a aflat despre acestea dintr-o singură sursă, foarte importantă; în caz contrar, nu ar fi acţionat atât de ostentativ, deoarece acest lucru ar fi pus sursa în pericol. Potrivit lui Ames, cei de la KGB care se ocupau de el au recunoscut că decizia KGB îl punea în pericol; i-au comunicat că

”regretau faptul că l-au pus într-o asemenea situație, dar conducerea politică nu a avut de ales”. Comisia senatorială privind activitatea serviciilor de informații, *An Assessment*, 25.

72. Comisia senatorială privind activitatea serviciilor de informații, *An Assessment*, 46-53. Clayton Lonetree, un puşcaş marin care asigura paza ambasadei SUA din Moscova a avut o relație cu o rusoaică care lucra la KGB. Un coleg a declarat inițial (dezmințind ulterior) că Lonetree i-a permis KGB-ului să pătrundă în clădirea ambasadei americane. Acest incident a produs confuzie în cadrul anchetei şi a distras atenția de la posibilitatea – pe care CIA se temea oricum să o ia în considerare - ca sursa problemelor să fi fost un ofițer CIA.

73. Comisia senatorială privind activitatea serviciilor de informații, *An Assessment*, 64-66. Din diferite motive, acest pont primit în noiembrie 1989, nu a fost exploatat suficient; Ames a fost arestat abia în luna februarie 1994.

CAPITOLUL 6: PĂZINDU-I PE GARDIENI: MANAGEMENTUL INFORMAȚIILOR

1. Deşi senatorul Church, preşedintele Comisiei senatoriale înființate în 1975 pentru investigarea activității serviciilor de informații, a folosit termenul de “oaie rătăcită” la începutul investigației pentru a desemna CIA-ul; această caracterizare a fost abandonată până la încheierea investigației. Conform lui Loch Johnson, un membru al comisiei Church care simpatiza cu senatorul Church, explica faptul că preşedintele comisiei folosise acest termen deoarece ”avea sentimentul că impactul probelor trebuia exagerat pentru a avea efect asupra publicului,” în timp ce raportul final al comisiei “evita cu grijă teoria <oii rătăcite>.”Loch Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* (Lexington: University Press of Kentucky, 1985), 224, 268.

2. Comisia senatorială privind operațiunile guvernamentale referitoare la activitățile de culegere de informații, *Alleged Assassination Plots Involving Foreign Leaders: Interim report*, al 94-lea Congres, prima sesiune, 1975, S. Rept 94-94, 263.c.

3. Pe 7 mai 1962, procurorul general Robert F. Kennedy a fost informat oficial cu privire la acțiunile întreprinse între 1960 şi 1961 în vederea asasinării lui Castro, subliniindu-se implicarea CIA în acest sens alături de doi membri ai Mafiei John Roselli şi Sam Giancana. Necesitatea unei achete oficiale a survenit din cauza faptului că FBI-ul intenționa să îl pună sub acuzare pe Robert Maheu, omul de legătură dintre CIA şi Mafie, pentru instalarea de dispozitive de interceptare ilegale iar CIA dorea să împiedice această măsură pentru ca întreaga poveste să nu fie dezvăluită. Se spune că Kennedy s-a fi înfuriat aflând de implicarea Mafiei, ceea ce ar fi complicat punerea sub acuzare a lui Roselli sau Giancana pentru posibile acte de crimă organizată; se pare că nu ar fi fost la fel de furios când a aflat de încercarea de asasinat. Comisia specială, *Alleged Assassination Plots*, 131-34.

4. Cea mai bună dovadă în acest sens o reprezintă faptul că membrii administrației nu s-au arătat deloc indignați atunci când operațiunile împotriva lui Castro au devenit publice. În mod evident, aceasta este o atitudine de genul “nici usturoi nu a mâncat…”; cu toate acestea, era de aşteptat ca membri

importanți ai administrației Kennedy, cum ar fi fostul Secretar al Apărării Robert McNamara, să se arate iritați de faptul că CIA s-a implicat în astfel de activități fără să primească aprobare de mai sus. În schimb, McNamara a subliniat, în fața comisiei Church, că după părerea sa "CIA era o organizație extrem de disciplinată, perfect controlată de importanți membri ai guvernului" (Comisia Specială, *Alleged Assassination Plots*, 159, citând depoziția lui McNamara din 11 iulie 1975). Se pare că reacția lui Robert Kennedy din 1962 a fost similară; vezi nota anterioară.

5. Christopher Andrew, *Her Majesty's Secret Service: The Making of the British Intelligence Community* (New York: Viking, 1986), 1.

6. Wiston S. Churchill, *Marlborough: His Life and Times* (New York: Scribner, 1938), vol. 6, 482-84 şi 526 –29. Oponenții lui Marlborough susțineau că acești bani reprezentau fonduri publice şi trebuia să se dea socoteală pentru ei ținându-se cont de acest lucru; datorită faptului că acesta a folosit fondurile pentru a-şi plăti agentura, acest lucru ar fi fost imposibil. Churchill susține cu tărie că ilustrul său strămoş a procedat corect folosind sursele tradiționale de bani pentru a finanța activitățile de culegere de informații, care nu erau finanțate de guvern.

7. La începuturile republicii americane s-a încercat aproximarea vechiului sistem, Congresul stabilind un fond pentru situații neprevăzute aflat la discreția preşedintelui care să poată fi folosit pentru a plăti persoanele care "servesc SUA în afara teritoriului țării." Preşedintele era obligat să informeze Congresul numai despre faptul că banii au fost cheltuiți; nu trebuia divulgat nici scopul plăților şi nici numele celor care primeau aceste plăți. Primii preşedinți recurgeau la persoane private care desfăşurau anumite afaceri peste hotare; acești "agenți" erau numiți fără aprobarea Senatului. În privința înființării fondului şi despre modul în care erau utilizați acești agenți, vezi Stephen F. Knott, *Secret and Sanctioned: Covert Operations and the American Presidency* (New York: Oxford University Press, 1996), 49-60.

8. Prevederile au apărut inițial în deciziile prin care se hotăra înființarea comisiilor privind activitatea serviciilor de informații din Senat şi din Camera Reprezentanților şi au fost formulate sub forma unei legi în 1980; cu schimbări miniore acestea au devenit Legea autorizării informațiilor secrete din 1991. Prevederile de interes sunt reprezentate de secțiunile 501 şi 502 din Legea privind securitatea națională din 1947.

9. Robert M. Gates, " The CIA and American Foreign Policy", *Foreign Affairs* 66, nr. 2 (iarna 1987 - 88): 225. Potrivit acesteia, "Congresul a primit peste 1000 informări ale CIA şi 7000 rapoarte de informații în 1991." Loch K. Johnson, "Smart Intelligence*," Foreign Policy*, nr. 89 (iarna 1992-93): 67. În anii '90 tendința a continuat: În Legea autorizării informațiilor secrete din 1990 (PL101-193, 30 noiembrie 1989) a stabilit ca numirea inspectorului general (IG) al CIA să fie confirmată de Senat. În plus, legea prevedea ca directorul CIA să înaiteze comisiilor de supraveghere copii ale rapoartelor bianuale ale IG. Prin urmare, în 1999 Legea autorizării informațiilor secrete (PL105-272, 20 octombrie 1998), Congresul a adoptat o serie de prevederi menite să îi protejeze pe aşa – numiții "informatori" din comunitatea de informații. Legea prevede o serie de proceduri prin care angajații serviciilor secrete pot furniza informații în situații speciale comisiilor de supraveghere prin inspectorul general al serviciului şi prin director. Vorbind despre această măsură,

preşedintele comisiei din Camera Reprezentanţilor a precizat, “Am deschis o uşă pentru a înlesni schimbul de informaţii cu Congresul.” *Congressional Record*, 7 octombrie 1997, H9729.

10. Realitatea acestui “domeniu privat” a fost întărită de teoriile de administraţie publică, care subliniau distincţia dintre ”realitate şi valoare”, încercau să facă o distincţie înte cei care elaborau politicile şi componenta birocratică (administraţia) a căror datorie era implementarea unei politici în modul cel mai eficient şi mai raţional. Pentru varianta americană tradiţională a acestei teorii, vezi Woodrow Wilson, “ The Study of Administration”, *Political Science Quarterly* 2 (iunie 1887): 197 – 222. Puţini specialişti din acest domeniu mai iau în considerare această diferenţă în ziua de azi, dar rămâne în continuare (în absenţa unui punct de vedere alternativ coerent) principala teorie printre cei din administraţie, dar şi printre cei ce urmăresc reformarea administraţiei.

11. Într-o mai mică măsură, această teorie de organizare este reflectată de decizia Marii Britanii din 1983 ca preşedintele Comisiei mixte pentru activitatea de informaţii (JIC, agenţia guvernamentală britanică responsabilă cu coordonarea activităţii de culegere de informaţii şi a evaluărilor la nivel naţional) să fie numit de primul ministru din rândul echipei guvernamentale; anterior, preşedintele fusese ales din rândul angajaţilor Ministerului de Externe. Schimbarea recomandată de o comisie de anchetă (Comisia Franks) însărcinată cu evaluarea activităţii serviciilor secrete britanice în timpul crizei Falklands avea drept scop să îi confere preşedintelui JIC un “rol mai important şi mai multă independenţă”. Pentru mai multe detalii privind ancheta Comisiei Franks vezi Robert Cecil, “The Assessment and Acceptance of Intelligence: A Case-Study,” în *British and American Approaches to Intelligence*, editată de K.G. Robertson (Londra: Macmillan, RUSI Defense Studies Series, 1987), 166-83.

    În mod similar, avântul iniţial pentru crearea Agenţia de informaţii a armatei americane (DIA) putea fi atribuit, cel puţin parţial, dorinţei de a înfiinţa (în cadrul Departamentului de Apărare) o agenţie centralizată de evaluare care să fie independentă de vederile înguste şi interesele serviciilor militare şi a agenţiilor acestora de informaţii. Pentru mai multe detalii privind efortul mai mult decât neizbutit de a înfiinţa DIA conform acestor principii, vezi Patrick Mescall, “The birth of the defense Intelligence Agency”, în *North American Spies: New Revisionist Essays*, editată de Rhodri Jeffreys-Jones şi Andrew Lownie, (Lawrence: University Press of Kansas, 1991), 158-201.

12. Graham E. Fuller, “Intelligence, Immaculately Conceived,” *The National Interest*, nr.26 (iarna 1991-92):98.

13. *Antony and Cleopatra*, 2.5.85-88.

14. Cel mai renumit teoretician militar, Carl von Clausewitz, care se arăta foarte sceptic în privinţa acurateţii şi a valorii majorităţii rapoartelor de informaţii considera că un comandant trebuia să dea dovadă de capacitatea de defini clar obiectivele activităţii desfăşurate: “Comandantul trebuie să aibă încredere în judecata sa şi să fie ca o stâncă într-o mare [de informaţii false].” Carl von Clausewitz, *On War*, editată şi tradusă de. Michael Howard şi Peter Paret (Princeton N.J.: Princeton University Press, 1976), 117.

15. Henry Brandon, *The Retreat of American Power* (New York: Doubleday, 1973), 103. Se spune că preşedintele Johnsons a făcut această remarcă la o cină la Casa Albă în compania Directorului Richard Helms.

16. "Managing/ Teaching New Analysts," *Studies in Intelligence* 30, nr. 3 (toamna 1986): 3-4. Numele autorului (se pare un director din cadrul Directoratului pentru informații secrete, CIA) a fost șters ca răspuns la o cerere înaintată pe baza Legea privind accesul liber la informații. Îi sunt recunoscător lui Eliot Cohen pentru că mi-a atras atenția în privința acestui articol. Acesta discută articolul în "Analysis," în *Intelligence Requirements for the 1990s: Collection, Analysis, Counterintelligence and Covert Action*, editată de Roy Godson (Lexington, Massachussets: Heath, Lexington, 1989), 71-96.

17. Cohen, "Analysis," 76.

18. Charles H. Fairbanks Jr., "Where is the Secret?" *Washington Post*, 25 februarie 1987, A23 [subliniere în original].

19. Fairbanks, "Where Is the Secret?"

20. Fuller, "Intelligence Immaculately Conceived," 96-97. Cu toate acestea, pentru Fuller caracterul ideologic inerent al analizei informațiilor secrete strategice nu pare să aibă niciun fel de implicații în ceea ce privește relația dintre informațiile secrete și strategie. Îndeosebi, acesta nu pare să fie de acord cu opinia factorilor de decizie conform căreia strategia bazată pe informații secrete poate submina strategia administrației (vezi nota 12 de pe pagina anterioară). Din punctul de vedere al unui analist de informații secrete, Fuller pledează pentru independență (posibilitatea de a putea ignora poziția factorilor de decizie), dar nu abordează argumentele care ar putea justifica acest lucru.

21. Bob Woodward și Dan Morgan, "Soviet Threat toward Iran Overstated, Casey Concluded," *Washington Post*, 13 ianuarie 1987, A1.

22. Loch K. Johnson, *Secret Agencies: U.S. Intelligence in a Hostile World* (New Haven, Connecticut: Yale University Press, 1996), 129.

23. Robert M. Gates, "The CIA and Foreign Policy," *Foreign Affairs 66*, nr.2, (iarna 1987-88): 221.

24. Această secțiune se bazează pe lucrearea lui Abram N. Shulsky și Gary Schmitt, *The Future of Intelligence: Report Prepared for the Working Group on Intelligence Reform* (Washington, D.C.: Consortium for the Study of Intelligence, 1996), 14-16.

25. Legea securității naționale din 1947, sect. 501 (a) (1), conform amendamentelor [50 USC 413].

26. Gates, "The CIA and Foreign Policy," 225.

27. Legea privind controlul activității de informații din 1980 menționa clar că "prevederea anterioară nu va necesita aprobarea din partea comisiilor pentru controlul activității de informații anterior inițierii unei astfel de activități de informații [operațiune secretă]." Legea autorizării informațiilor secrete din 1991, care revedea cerințele privind raportarea operațiunilor secrete în fața Congresului, prevedea o solicitare similară. Legea securității naționale din 1947, conform amendamentelor, sect. 501 (a) (1), [50 USC 413 (a)(3)]. O astfel de ocazie când comisiile și-au exercitat dreptul de veto a apărut legat de o propunere a administrației Bush din 1989 de a asigura ajutor secret forțelor potrivnice lui Noriega în Panama. Vezi Stephen Engleberg, "*U.S. Officials Say Senators Balked At Noriega Ouster*," New York Times, 24 aprilie 1989, A1.

28. Un alt exemplu al folosirii fățișe a puterii financiare în detrimentul operațiunilor secrete îl reprezintă asistența acordată rezistenței anticomuniste din Cambodgia. În Conference Report ce însoțea Legea autorizării informațiilor secrete din 1991 înaintat în octombrie 1990, cele două comisii pentru controlul activității de informații au precizat pe larg tipul de aistență ce urma să fie acordat (neletal) şi în ce scop (promovarea unui acord de pace). Comisia permanentă privind activitatea serviciilor de informații din Camera Reprezentanților SUA, *Conference Report: Intelligence Authorization Act for Fiscal Year 1991*, 101 Congres, sesiunea a doua, Raportul Camerei Reprezentanților 101-928, 34. Congresul a blocat cererea administrației Bush de alocare de fonduri pentru ajutor militar letal către forțele anticomuniste din Cambodgia. Peter Rodman, "Supping with Devils," *The National Interest*, nr. 25, (toamna 1991):47.

29. Datele despre scurgerile de informații sunt nu numai rare, dar pot, totodată, induce în eroare. Referirea într-un articol la o "sursă din Congres" sau la "un funcționar din adminstrație" nu va indica neapărat sursa jurnalistului; sursa originală a făcut practic imposibilă orice referire la ea. Astfel referirea din articol poate trimite către o sursă care a comentat pe marginea unor aspecte dintr-o informație deja deținută de jurnalist şi nu la sursa originală. Leon V. Sigal, *Reporters and Officials: The Organization and Politics of Newsmaking* (Lexington, Massachussets: Heath, 1973) discută pe marginea acestor tactici care permit unui funcționar "să își asigure un alibi".

30. Comisia senatorială privind operațiunile guvernamentale referitoare la activitățile de culegere de informații [de aici înainte cunoscută sub numele de Comisia Church], *Final Report*, vol. I : *Foreign and Military Intelligence*, Congres 94, sesiunea a doua, 1976, S. Rept. 94.755, 522. Halperin susținea abolirea dreptului de a desfăşura operațiuni secrete.

31. După cum a remarcat Samuel Huntington:

    Într-o atmosferă diferită…comisiile din Congres care investigau acitivitatea CIA ar fi putut arăta curiozitate în privința eşecului Agenției de a-i asasina pe Lumumba şi Castro…[cu toate acestea, la momentul respectiv], nimeni nu era interesat dacă Agenția avea capacitatea de a îndeplini ordinele primite, singurul lucru care suscita interes era caracterul imoral al ordinelor primite.

    Huntington, *American Politics: The Promise of Disharmony* (Cambridge, Massachussets: Harvard University Press, 1981), 191.

32. Pentru o prezentare a sistemului canadian, vezi Geoffrey R. Weller, "Accountability in Canadian Intelligence Services," *International Journal of Intelligence and Counterintelligence 2*, nr. 3 (toamna 1988): 415 - 41 şi Reg Whitaker, "The Politics of Security Intelligence Policy-making in Canada: II, 1984," *Intelligence and National Security 7*, nr. 2 (aprilie 1992): 53 - 76.

33. Vezi Frank Cain, "Accountability and the Australian Security Intelligence Organization: A Brief History," în *Security and Intelligence in a Changing World: New Perspectives for the 1990s*, editată de A. Stuart Farson, David Stafford şi Wesley K. Wark (Londra: Frank Cass, 1991), 10-24, 104 - 25.

34. În general, foarte puține informații au fost făcute publice privind supravegherea activității de informații în alte țări decât cele deja menționate. Deşi au apărut noi reglementări privind activitatea de supraveghere în mai multe țări, s-au publicat destul de puține lucrări care descriu şi compară diverse sisteme de

supraveghere. Alfred B. Prados şi Richard A. Best, "Intelligence Oversight in Selected Democracies,"CRS Rept. 90 483, Departamentul de cercetare al Congresului, Biblioteca Congresului, 21 septembrie 1990, deşi o publicație mai veche, aceasta rămâne o sursă valoroasă pe acest subiect.

35. Legea privind activitatea serviciilor secrete 1994, sect. 10(3), citată de Comisia specială pe probleme interne din Camera Comunelor, *Third Report: Accountability of the Security Service*, 14 iunie 1999. Raportul este disponibil şi pe www.fas.org/irp/world/uk/docs/291/29102.htm.

36. Camera Comunelor, *Third Report*. Sistemul de supraveghere din Noua Zeelandă conferă primului ministru puteri sporite. În 1996 în urma Legii de înființare a comisiei pentru siguranță şi controlul activității de informații a luat naştere comisia de supraveghere a activității de informații cu următoarea componență: primul ministru, liderul opoziției, doi membri ai Parlamentului aleşi de premier şi un membru al opoziției ales de liderul opoziției. Deşi mandatul extins al comisiei prevede "examinarea strategiei, modului de administrare şi a cheltuielilor fiecărui serviciu de informații şi securitate", autoritatea sa de supraveghere este limitată de faptul că premierul şi cei numiți de acesta dețin majoritatea în comisie iar premierul este singurul care poate solicita audieri. În plus, comisia nu are dreptul să investigheze "nicio problemă sensibilă din punct de vedere operativ, inclusiv orice problemă legată de culegerea de informații şi metodele producere şi sursele informațiilor." Legea poate fi găsită pe internet la rangi.knowledge-basket.co.nz./gpacts/public/text/1996/se/046sel.html.

37. Site-ul Parlamentului australian: www.aph.gov.au/house/committee/pjcasio/ppgrole.htm.

38. "Dreptul oamenilor de a fi protejați …împotriva unor anchete şi confiscări de bunuri nemotivate, nu va fi încălcat şi nu vor fi emise mandate, decât în cazuri justificate." Constituția SUA, al patrulea amendament.

39. P.L. 95-511 [50USC 1801-11]. Pentru o prezentare a legii şi a elaborării acesteia, vezi Americo R. Cinquegrana, "The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978," *University of Pensylvania Law Review* 137 (ianuarie 1989): 793 – 828 şi Elizabeth B. Bazan, "The Foreing Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance," Departamentul de cercetare al Congresului, Biblioteca Congresului, 17 mai 2000.

40. Legea autorizării informațiilor secrete din 1995 (P.L 103-359, 14 octombrie 1994), sec. 807. "anchetă fizică" este definită ca fiind "orice pătrundere… în spații sau pe proprietate…care are drept scop confiscarea…sau alterarea unor informații, materiale sau bunuri, în condițiile în care persoana respectivă are dreptul la o viață privată, un mandat fiind necesar în scopul punerii în aplicare a legii, dar nu include [informații obținute din transmisii radio-electronice]."

41. Într-un studiu detaliat numit "The Study of Intelligence in the United States," Kenneth G. Robertson remarcă: "Până în prezent s-a cercetat destul de puțin natura amenințărilor interne şi modul în care acestea pot influența cerințele privind informațiile secrete obținute de pe teritoriul țării." În *Comparing Foreign Intelligence: The U.S., the USSR, the UK and the Third World*, editată de Roy Godson (McLean, Vancouver: Pergamon-Brassey's, 1988), 19. Situația nu s-a schimbat semnificativ de la publicarea studiului lui Robertson.

42. Desigur, nu toate infracţiunile sunt importante din punct de vedere al informaţiilor secrete obţinute de pe teritoriul ţării; standardul infracţional nu stabileşte ceea ce ar fi de interes pentru activitatea de culegere de informaţii de pe teritoriul ţării, ci mai degrabă ceea ce nu face obiectul acestei activităţi. În general, culegerea de informaţii legată de activitatea de punere în aplicare a legii vizează mai degrabă crima organizată – Mafia şi activităţile gangsterilor, traficul de droguri pe scară largă – mai degrabă decât actele infracţionale sporadice.

43. Potrivit acelui act, supravegherea electronică a "persoanelor cu cetăţenie americană" (cetăţeni sau persoane de origine străină cu drept de reşedinţă permanent) este permisă doar dacă există "motive întemeiate" pentru a suspecta persoana respectivă că este implicată cu bună ştiinţă în acte de sabotaj în favoare unei puteri străine, terorism internaţional sau alte activităţi clandestine de culegere de informaţii care presupun violarea legii penale.

44. O variantă adaptată a acestor principii a fost elaborată în urma unei cereri pe baza Legea privind libertatea informaţiilor şi a apărut în Comisia senatorială privind activitatea serviciilor de informaţii, *National Intelligence Reorganization and Reform Act of 1978: Hearings*, Congres 95, ses.2, Committee Print, 774-90.

45. Comisia senatorială privind activitatea serviciilor de informaţii, Hearings, paragraf II A, 775 [sublinere în original]

46. Lege Înregistrării Agenţilor Străini din 1938 prevede: deconspirarea numelor persoanelor implicate în activităţi de propagandă sau alte tipuri de activităţi pentru sau în numele unor ţări străine astfel încât guvernul şi cetăţenii Statelelor Unite să poată fi informaţi cu privire la identitatea acestor persoane, putându-le evalua afirmaţiile şi acţiunile în strânsă legătură cu mediile frecventate şi activităţile derulate.

    Citatul este extras din legea mai sus menţionată, secţiunea privind "Politica şi obiectivele". Legea în sine, exceptând această afirmaţie, este criptată la 22 USC 611-21.

47. Pe 9 februarie 1989, Alan Thomson, directorul Consiliului Naţional al Prieteniei Americano-Sovietice, a fost arestat după constituirea unui depozit bancar de 17.000 de dolari în bani lichizi. Se pare că suma ar fi fost furnizată de Asociaţia Sovietică pentru Prietenie şi Relaţii Culturale cu alte state, care, potrivit unui raport FBI, se afla sub controlul Departamentului Internaţional al Comitetului Central al Partidului Comunist din Uniunea Sovietică. Aceasta fiind prima decizie de punere sub arest din Statele Unite, corelată cu măsuri eficiente sau misiuni secrete ale Uniunii Sovietice, acuzaţia propriu-zisă s-a bazat mai curând pe nedeclararea acestor transferuri importante de bani (conform prevederilor referitoare la combaterea activităţilor de spălare a banilor) decât pe neînregistrarea persoanei în cauză ca cetăţean străin. (Associated Press, 8 februarie 1989, *Washington Post*, 8 februarie 1989, A4). În mai 1992, Thomson a recunoscut că se face vinovat pentru nedeclararea banilor la intrarea în Statele Unite, după cum stipulează reglementările vamale în vigoare. Dan Herbeck, "Man Fined 1000 Dollars for Not Declaring Cash", *Buffalo News*, 31 iulie 1992 (secţiunea cu ştiri locale).

48. Comisia Senatorială pentru Serviciile Secrete din SUA, *The FBI and CISPES: Report*, Congresul 101, sesiunea 1, Raportul Senatului 101-46, 21. O anchetă amănunțită a CISPES a fost inițiată ulterior de FBI pe temeiuri complet diferite.

49. În 1983, Levi Domestic Security Guidelines a fost înlocuit cu "Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations", aprobat de Procurorul General William French Smith. Textul ambelor lucrări se poate regăsi în ediția Roy Godson, *Intelligence Requirements for the 1980s: Domestic Intelligence* (Lexington, Mass.: Heath, 1986), 225-64. Pentru o privire de ansamblu asupra lucrării lui Smith şi a compatibilității cu lucrarea lui Levi, vezi John T. Elliff, "The Attorney General's Guidelines for FBI Investigations", *Cornell Law Review* 69, nr. 4 (aprilie 1984): 785-815.

50. Levi, Domestic Security Guidelines, paragraf I.A., în *Domestic Intelligence*, ed. Godson, 225.

51. Lucrarea lui Levi nu face o referire clară la acest aspect; în schimb, în lucrare se precizează că "toate anchetele derulate în conformitate cu reglementările conținute în această lucrare vor fi inițiate şi conduse astfel încât să nu impieteze exercitarea deplină a drepturilor prevăzute prin Constituția şi legislația Statelor Unite" (paragraful II B). Astfel, nu se ştie exact dacă ancheta propriu-zisă restrânge dreptul la liberă exprimare prin descurajarea acesteia; de aceea, o anchetă bazată numai pe ideea protejării dreptului la exprimare al unui individ sau al unei grupări ar încălca această prevedere.

    În acest context, unul dintre cele mai controversate aspecte legate de lucrarea lui Smith l-a constituit prevederea potrivit căreia FBI-ul poate demara o anchetă numai în baza unor afirmații care "sprijină infracționalitatea sau care indică o intenție aparentă de a comite o infracțiune". În schimb, lucrarea lui Levi nu face nicio referire la anchetele bazate numai pe acest gen de afirmații. Cu toate acestea, după cum s-a putut vedea şi din citatul de mai sus, afirmațiile care ar putea prezenta interes în derularea anchetei sunt stabilite în funcție de standardele de infracționalitate prevăzute în lucrarea lui Smith.

52. *Laird v. Tatum*, 408 U.S. 1 până la (1972), 13-14.

53. Robertson, "The Study of Intelligence in the United States", 18-21.

54. Brandenburg v. Ohio, 395 U.S. 444 până la 447 (1969) [sublinierea adăugată].

55. Scales v. United States, 367 U.S. 203 până la 220 (1961). Curtea Supremă parafrazează şi (în cazul afirmațiilor plasate între ghilimele) citează recomandările judecătorului în fața juriului; ulterior, Curtea Supremă aprobă aceste recomandări (224).

56. John T. Elliff, *The Reform of FBI Intelligence Operations* (Princeton, N.J.: Princeton University Press, 1979), 57.

57. Desigur, gruparea ar trebui să aibă o capacitate de autocontrol extraordinară pentru a nu comite acte de violență sau alte acte prin care se încalcă legea, în perioada în care încearcă să se infiltreze în Guvern. Se pare că grupările de extremă dreapta care activează în prezent în Statele Unite şi în alte state democratice nu sunt atât de experimentate.

58. Shlomo Gazit şi Michael Handel, "Insurgency, Terrorism and Intelligence", în *Domestic Intelligence*, editura Godson, 134.

59. Standardele stabilite ("limitările") diferă de la o lucrare la alta. Potrivit lui Levi, FBI-ul nu poate folosi un informator decât dacă are "dovezi palpabile care să probeze faptul că… o grupare este sau ar putea fi implicată în activităţi ce presupun recurgerea la forţă sau violenţă şi care implică sau ar putea implica încălcarea legii federale" (secţiunea II [I], 227-28. Potrivit lui Smith, într-o anchetă "preliminară" poate fi folosit un informator cu aprobarea agentului numai în caz de necesitate sau dacă alte metode de investigaţie mai puţin invazive nu sunt eficiente. O "anchetă preliminară" poate fi demarată în cazul în care FBI-ul primeşte informaţii privind o posibilă infracţiune care, chiar dacă "nu impune o anchetă detaliată", presupune o serie de eforturi în scopul verificării pistelor iniţiale (secţiunea II [B](1)(6), 248-51).

60. Acest citat, precum şi următoarele două, sunt extrase din "Discussion" de John M. Walker Jr., în *Domestic Intelligence*, ed. Godson, 194-96.

61. Lucrarea Procurorului General (Smith), Guidelines on Domestic Security, III.B.1(a), în *Domestic Intelligence*, ef. Godson, 258.

62. David M. Park, "Re-examining the Attorney General's Guidelines for FBI Investigations of Domestic Groups", *Arizona Law Review* (vară 1997): 774, citează mărturia lui Freeh în faţa Camerei Reprezentanţilor, a Comisiei pentru Relaţii Internaţionale, Subcomisiei pentru Investigarea Infracţiunilor, *Terrorism Hearings*, Congresul 104, sesiunea 1, 1995, 12.

63. Lucrarea lui Smith, III.B.1(a), în *Domestic Intelligence*, editura Godson, 258.

64. Mărturia lui Laurence H. Silberman, 18 iulie 1978 în faţa Comisia Senatorială pentru Serviciile Secrete din SUA, *Hearings*, 616.

65. Comisia Church, Final Report, cartea 2: *Intelligence Activities and the Rights of Americans*, Congresul 94, sesiunea 2, 1976, Raportul Senatului 94-755, 166. Odată cu publicarea lucrării lui Levi, numărul anchetelor pe tema securităţii interne a scăzut semnificativ. În aprilie 1976, au fost demarate 4868 de anchete; până la sfârşitul lui septembrie, au fost iniţiate numai 626. În august 1982, erau în curs de desfăşurare numai 38 de anchete privind securitatea internă. Senatul American, Subcomitetul pe probleme de Securitate şi Terorism, Comitetul Juridic, *Impact of Attorney General's Guidelines for Domestic Security Investigations (The Levi Guidelines): Hearing*, Contresul 98, sesiunea 1, 1983, Raportul Senatului 98-134, 5.

66. Comisia Church, *Raportul Final*, cartea 2, 225-40, face referire la cazurile ce au furnizat informaţii strict politice, care au fost trimise factorilor de decizie din domeniul administrativ.

67. Legea privind Activitatea Serviciilor Secrete Canadiene, 1984, secţiunile 2 şi 12. Potrivit legislaţiei canadiene, atribuţiile de culegere şi analiză a informaţiilor secrete privind ameninţările la adresa securităţii, precum şi cele de evaluare a personalului din sfera securităţii revin Serviciului Secret de Informaţii Canadian şi Securitate, în timp ce Poliţia Călare Canadiană este responsabilă cu aplicarea legislaţiei referitoare la securitatea naţională şi garantarea protecţiei şi securităţii guvernanţilor şi a obiectivelor guvernamentale. Puteţi găsi această lege www.csis-scrs.gc.ca/end/act/csisact_e.html.

CAPITOLUL 7: DOUĂ PERSPECTIVE ASUPRA SERVICIILOR DE INFORMAȚII

1. Sun Tzu, *The Art of War*, traducere de Samuel B. Griffith (Oxford: Oxford University Press, 1964), 144-45 (capitolul 13, paragrafele 3-4). "Tzu" este varianta romanizată (transcrisă în alfabet latin) învechită, dar familiară a unui personaj chinezesc care s-ar traduce, în zilele noastre, prin "Zi".
2. Sun Tzu, *The Art of War*, 146 (capitolul 13, paragrafele 9-10).
3. Sun Tzu, *The Art of War*, 77-78 (capitolul 3, paragrafele 4-6). Acest punct de vedere contrastează cu cel al lui Carl von Clausewitz, care consideră că anihilarea forțelor de luptă inamice este esențială. Carl von Clausewitz, *On War*, publicată şi tradusă de Michael Howard şi Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 90 (cartea 1, capitolul 2). După cum s-a putut remarca, Clausewitz se arată mult mai sceptic în privința şansei ca informațiile secrete să permită implicarea unui comandant în misiuni grele, care să se finalizeze cu o victorie şi să implice costuri minime. Acesta afirmă că "pe scurt, majoritatea informațiilor secrete sunt false" (117, cartea 1, capitolul 7).
4. William E. Colby, "Intelligence in the 1980s", *The Information Society* 1, nr. 1 (1981): 53-54.
5. Colby, "Intelligence in the 1980s", 65.
6. Pe 11 iulie 1941, preşedintele Roosevelt a decretat înființarea "Departamentului de Informații Secrete, cu atribuții de culegere şi analiză a informațiilor şi datelor ce ar putea aduce atingere securității naționale, atribuții de procesare a acestor informații şi date, precum şi de informare a preşedintelui, a ministerelor şi a oficialilor abilitați de preşedinte să le cunoască…" (Decretul prezidențial "Designating a Coordinator of Information", paragraful 1). Decretul a fost republicat în cartea lui Thomas F. Troy, *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency* (Frederick, Md.: University Publications of America, 1981), 423.
7. Colby, "Intelligence in the 1980s", 54.
8. Vezi Ray S.Cline, *The CIA: Reality vs. Myth*, ediția revizuită (Washington, D.C.: Acropolis, 1982), 78, 80-81, pentru o polemică privind incapacitatea de procesare şi de analiză a Departamentului OSS care se ocupă de partea analitică a operațiunilor CIA. Cline precizează că "[nicio] componentă a OSS nu a folosit vreodată în rapoartele sale informații obținute din transmisii radio-electronice" (78). De aceea, nu a avut acces la majoritatea surselor de informații secrete (Ultra şi Magic) aflate la dispoziția Guvernului Statelor Unite.
9. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, N.J.: Princeton University Press, 1949; republicată cu o nouă prefață, 1966), 155. Recomandările lui Kent referitoare la serviciile de informații au fost acceptate din două motive. Aşa cum Berkowitz şi Goodman au subliniat, "*Strategic Intelligence* a fost probabil cea mai inspirată carte despre analiza informațiilor secrete scrisă vreodată. A devenit o lucrare de referință nu numai pentru studenții americani care doreau să devină ofițeri de informații, ci şi în afara granițelor, fiind ulterior tradusă în franceză, rusă, germană şi în alte

limbi." În plus, după eşecul comunităţii serviciilor de informaţii, care nu a reuşit să împiedice, în 1950, invadarea Coreei de Sud de către Coreea de Nord, Walter Smith (zis "Beedle"), directorul agenţiei, a solicitat înfiinţarea "unui nou departament care să se ocupe de evaluarea dinamică şi minuţioasă a informaţiilor secrete. Aceste rapoarte au devenit cunoscute sub numele de Evaluări Informative Naţionale (NIE), iar instituţia s-a numit Biroul pentru Evaluări Informative Naţionale (ONE)." Kent a fost desemnat primul director adjunct al ONE, iar în 1952 a devenit directorul Biroului, poziţie pe care şi-a păstrat-o timp de 16 ani. "Nu este nevoie să mai spun", au precizat Berkowitz şi Goodman, "că ONE şi modul de realizare a rapoartelor se aseamănă, într-o mare măsură, principiilor analitice descrise de Kent în *Strategic Intelligence*". Bruce D. Berkowitz şi Allan E. Goodman, *Strategic Intelligence for American National Security* (Princeton, N.J.: Princeton University Press, 1989), 4-5.

10. Kent, *Strategic Intelligence*, 3-4 [sublinierea autorului].

11. Colby, "Intelligence in the 1980s", 59. "Clubul de la Roma" a publicat, la sfârşitul anilor '70, o serie de studii despre tendinţele demografice, economice şi conjuncturale proiectate pentru secolul al XXI-lea. Previziunile clubului s-au dovedit extrem de pesimiste.

12. Potrivit lui Alexander Orlov, un defector al NKVD-ului sovietic (predecesorul actualului KGB), în contextul creat de Uniunea Sovietică, analiza sau evaluarea "ţine mai degrabă de stabilirea autenticităţii documentelor furate decât de importanţa informaţiilor. Importanţa politică a informaţiilor este evaluată mai întâi de factorii de decizie politici din cadrul Guvernului şi ai Prezidiului Executiv [Politbureau]." Alexander Orlov, *Handbook of Intelligence and Guerilla Warfare* (Ann Arbor: University of Michigan Press, 1965), 187.

    O polemică interesantă cu privire la importanţa analizei a pornit de la sistemul de radiolocaţie (DISTANT) pe care MI6 (serviciul de informaţii britanic) şi CIA i l-au pus la dispoziţie lui Oleg Penkovsky pentru a-l folosi în cazul în care ar fi intrat în posesia unor informaţii privind un atac iminent al Occidentului asupra Uniunii Sovietice. Potrivit unui studiu detaliat despre cazul Penkovsky, MI6 "se temea că un semnal de avertizare transmis prin intermediul sistemului de radiolocaţie DISTANT poate fi interpretat greşit sau poate conduce la ostilităţi, dacă nu este evaluat şi supravegheat cu atenţie." Marea Britanie era convinsă că orice avertizare ar trebui să fie mai întâi procesată de Comisia Mixtă pentru Activitatea de Informaţii (JIC), forul britanic superior de evaluare a informaţiilor, înainte de a ajunge la factorii de decizie politici. Potrivit unui reprezentant MI6 de la Washington, "un raport DISTANT nu ar trebui considerat de Marea Britanie ca o certitudine, decât în cazul în care JIC hotărăşte acest lucru." În schimb, opinia CIA, influenţată probabil de experienţa Pearl Harbor, a fost că mesajul ar trebui să parvină imediat factorilor de decizie politici; singura concluzie (deşi critică) rezultată de aici ar recomanda, înainte de toate, confirmarea sursei. Jerold L. Schecter şi Peter S. Deriabin, *The Spy Who Saved the World* (New York: Scribner, 1992), 284-86.

13. Eliot A. Cohen, "Analysis", în *Intelligence Requirements for the 1990s: Collection, Analysis, Counterintelligence and Covert Action*, edit. Roy Godson (Lexington, Mass.: Heath, Lexingont, 1989), 83.

14. Kent, "Preface to the 1966 Edition", *Strategic Intelligence*, xxiv.

15. Kent, "Preface", 58-59 [sublinierea în original].

16. Într-o anumită măsură, extinderea rolului analitic al serviciilor de informații din Statele Unite a fost rezultatul unei anomalii istorice datorate existenței unui adversar de talia Uniunii Sovietice în perioada postbelică. În timp ce alte țări consideră că este firesc să dea publicității anumite informații, rușii le tratează ca secrete de stat. În consecință, toate tipurile de informații care, altminteri nu ar fi fost decât simplă rutină și care, din punctul de vedere al tradiționaliștilor, nu ar fi de competența serviciilor secrete au devenit obiectul activității de culegere a informațiilor și, implicit, de analiză. Chiar dacă într-un mod diferit de teoriile lui Kent referitoare la natura strategică a informațiilor secrete, lipsa de deschidere a Uniunii Sovietice confirmă, la nivel concret, ideea că serviciile secrete sunt interesate de toate informațiile care au relevanță în plan strategic.

17. După cum am mai menționat, capitolul 6, secțiunea referitoare al "serviciile secrete imperiale".

18. Concepția despre importanța analizei informațiilor strategice și motivele care stau la baza acesteia a fost enunțată pentru prima dată de către Kent și colegii săi în cursul activității desfășurate în cadrul Departamentului de Cercetare și Analiză a OSS, în timpul celui de-al doilea război mondial. Potrivit istoricului Barry Katz, în fața ostilității acestei birocrații adânc înrădăcinate și

    în absența unei structuri stabile care să monitorizeze această activitate, singura modalitate de protecție aflată la îndemâna Departamentului [nou înființat] a fost vălul invizibil al obiectivității sociale… În mod surprinzător, ideea unei examinări atente a acestei obiectivități, bazată pe "o analiză generală a procesului de gândire științifică din sfera socialului", a fost susținută întotdeauna în timpul războaielor la care a fost martor aceste Departament. [În opinia lui Kent], poziția "oficială" s-a datorat mai ales acelor domenii de activitate la care cercetătorii americani din cadrul Departamentului de Cercetare și Analiză (R&A) se pricepeau cel mai bine, respectiv "acea sferă a științei cunoscută, în general, ca sociologie." În toate aceste discipline, antinomiile dintre fapt și valoare, erudiție și spiritul partizan cu care Max Weber s-a luptat cu atâta eroism au fost în mare parte estompate… a venit vremea sociologilor, a economiștilor și informaticienilor… Așa cum credibilitatea politică a Departamentului depindea de imaginea profesionalismului dezinteresat, credibilitatea epistemologică a disciplinelor se bazează pe o obiectivitate pozitivistă, care poate fi definită în teorie și doar aproximată în practică.

    Barry M. Katz, *Foreign Intelligence: research and Analysis in the Office of Strategic Services, 1942-1945* (Cambridge, Mass.: Harvard University Press, 1989), 14-15.

19. În februarie 1992, cele două comisii ale Congresului SUA pentru serviciile de informații au propus norme legislative care să reorganizeze din temelie comunitatea americană a serviciilor de informații. Unul dintre principalele proiecte de lege se referea la înființarea unei structuri centralizate de analiză, care să coordoneze toate instituțiile de analiză din cadrul comunității de informații. În plus, noul centru de analiză, creat după modelul unei structuri academice, ar fi independent de celelalte componente operative din cadrul comunității și de instituțiile guvernamentale care reprezintă factori de decizie

în stat. Potrivit preşedintelui Comisiei pentru Serviciile Secrete din cadrul Camerei Reprezentanţilor, congresmanul Dave McCurdy, reorganizarea a avut ca principal scop "crearea unui 'grup de experţi' de prim rang". "Intelligence Committee Chairmen Introduce Sweeping Reorganization plan", comunicatul de presă emis de Comisia Senatorială pentru Serviciile Secrete din SUA, 5 februarie 1992. Vezi şi David L. Boren, "The Intelligence Community: How Crucial", *Foreign Affairs* 71, nr. 3 (vară, 1992): 61. Senatorul Boren era, la vremea respectivă, preşedintele Comisiei Senatoriale pentru Serviciile Secrete şi susţinătorul propunerii legislative privind reorganizarea serviciilor de informaţii.

20. Vezi, de exemplu, recomandările lui Stansfield Turner incluse în memoriile sale despre activitatea în cadrul serviciilor secrete: *Secrecy and Democracy: The CIA in Transition* (Boston: Houghton Mifflin, 1985; New York: Harper and Row, 1986). După ce a lansat propunerea privind înfiinţarea unei Agenţii a Porţilor Deschise, care să furnizeze întregii lumi informaţii obţinute prin satelit, acesta a concluzionat:

    Capacităţile noastre din sfera serviciilor de informaţii sunt în deplină concordanţă cu rolul special pe care ni l-am asumat pentru apărarea propriei securităţi şi bunăstarea întregii omeniri, după ce ne-am revizuit propria concepţie despre necesitatea confidenţialităţii informaţiilor în cadrul proceselor democratice pe care se bazează guvernul nostru… Avem extraordinara şansă de a demonstra superioritatea sistemului nostru democratic, care îşi foloseşte capacităţile din domeniul serviciilor de informaţii nu numai în folosul propriei naţiuni, ci al întregii lumi şi umanităţi (285).

21. Colby, "Intelligence in the 1980s", 69.

22. Pentru o expunere care vine în sprijinul surselor secrete tehnice în această nouă eră, vezi capitolul 2, observaţia 86. Indiferent dacă sursele secrete tehnice sau cele umane vor avea întâietate în obţinerea informaţiilor secrete de importanţă deosebită în plan strategic, fără îndoială că, aşa cum s-a arătat în capitolul 2, sursele secrete tehnice – care încercau altădată să răspundă la cerinţele factorilor de decizie naţionali – vor avea un rol important în furnizarea informaţiilor secrete de ordin tactic comandanţilor de pe câmpul de luptă.

23. Kent, *Strategic Intelligence*, viii [sublinierea adăugată].

24. Referitor la acest aspect şi la probleme conexe, vezi Thomas F. Troy, "The 'Correct' Definition of Intelligence", *International Journal of Intelligence and Counterintelligence 5*, nr. 4 (iarnă, 1991092): 443-54.

25. Turner, *Secrecy and Democracy*, 279-85. Turner nu precizează dacă este dispus să pună la dispoziţia întregii omeniri mijloacele tehnice americane de culegere a informaţiilor sau informaţiile obţinute prin astfel de mijloace. Acesta afirmă că, pentru început, "am putea" [sublinierea adăugată] furniza numai "informaţiile obţinute cu ajutorul sistemelor perimate, care nu mai reprezintă o noutate" pentru adversar (282). Totodată, consideră că "nu peste mult timp fotografiile obţinute prin satelit vor fi atât de fidele încât diferenţele dintre diverse tipuri de sateliţi vor fi nesemnificative" (280).

26. Acest citat şi următorul sunt extrase din Colby, "Intelligence in the 1980s", 69.

27. Desigur, comiterea unui act de trădare la adresa unui regim tiranic sau agresiv poate fi justificată din punct de vedere moral. Pentru Ryszard Kuklinski, ofițerul din armata poloneză care a trecut de partea Statelor Unite și i-a spionat pe rușii ce îi asupreau țara natală, motivația era de ordin ideologic, astfel că ofițerii de informații din Vest nu au fost nevoiți să-l manipuleze sau să-l corupă în vreun fel. În alte cazuri, însă, când motivația o reprezintă banii sau spiritul de aventură, ofițerul de informații trebuie să exploateze punctele slabe ale potențialului spion pentru a-l determina să cedeze mai repede. Pentru o expunere mai detaliată pe marginea acestui subiect, vezi E. Drexel Godfrey Jr.,"Ethics and Intelligence", *Foreign Affairs 56*, nr. 3 (aprilie 1978): 624-42, și răspunsul lui Arthur L. Jacobs din "Comments and Correspondence", *Foreign Affairs 56*, nr. 4 (iulie 1978): 867-75.

28. Sun Tzu, *The Art of War*, 63-64 (capitolul 1, paragrafele 2-4).

29. Sun Tzu, *The Art of War*, 144 (capitolul 13, paragraful 2).

30. Henry L. Stimson și McGeorge Bundy, **On Active Service in Peace and War** (New York: Harper, 1948), 188. Probabil că Stimson nu a făcut această remarcă la vremea respectivă, ci și-a exprimat opinia ulterior, în timp ce-și justifica decizia legată de evenimentele din 1929, când "toată lumea făcea tot posibilul în direcția menținerii păcii, iar toate națiunile erau prietene", precum și pe cea de a sprijini (în calitate de secretar de stat pe probleme de război) cercetările în domeniul criptanalizei. Este puțin probabil, însă, ca al doilea război mondial să fi înregistrat atât de multe succese fără eforturile depuse în prealabil în această direcție. De exemplu, eforturile americanilor de a decoda mașina japoneză de criptat Purple, folosită pentru prima dată în 1939, au fost încununate de succes, depinzând în principal de decodarea mașinii de criptat Red, care data din 1931. Vezi Ronald Lewin, *American Magic: Codes, Ciphers and the Defeat of Japan* (New York: Farrar Strauss Giroux, 1982), 42-43. Pentru o privire de ansamblu asupra serviciilor de informații în perioada interbelică, vezi Robert G. Angevine, "Gentleman Do Read Each Other's Mail: American Intelligence in the Interwar Era", *Intelligence and National Security 7*, nr. 2 (aprilie 1992): 1-29.

31. Vezi, de exemplu, expunerea lui David Kahn pe această temă: "În cartea sa *Perpetual Peace*, Immanuel Kant susținea că spionajul este o crimă la adresa ordinii mondiale și că, dacă ar ieși la iveală, ar crea importante probleme internaționale. Dar acest lucru nu pare să se întâmple și în cazul SIGINT (informații obținute din interceptarea semnalelor și comunicațiilor electronice)." *Intelligence Requirements for the 1980s: Clandestine Collection*, editura Roy Godson (Washington, D.C.: Centrul Național de Informații Strategice, 1982), 120.

    În realitate, însă, dezvăluirea făcută în 1931 de Herbert Yardley, director al *American Black Chamber* (Camera Neagră), potrivit căreia Statele Unite au interceptat mesajele cifrate dintre Tokyo și delegația japoneză care a participat la conferința Forțelor Navale de la Washington privind limitarea marinei din punct de vedere militar (1921-22) a creat senzație în întreaga Japonie. *The American Black Chamber* (Indianapolis: Bobbs-Merrill, 1931; republicat, New York: Ballantine, 1981), 187-211.

    În mod asemănător, E. Drexel Godfrey Jr., fost ofițer CIA, susține că "sateliții de recunoaștere fotografică și vocală, precum și alte dispozitive de interceptare

sunt extrem de costisitoare, dar prezintă avantajul că aduc atingere numai într-o mică măsură standardelor etice ale angajaților şi angajatorilor". "Ethics and Intelligence", 637.

CAPITOLUL 8: ELEMENTE PENTRU O TEORIE A CULEGERII DE INFORMAȚII

1. După cum am precizat în Capitolul 1, prezentarea pe trei planuri a serviciilor de informații – informații, activitate şi structură – este extrasă din Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, N.J.: Princeton University Press, 1949; republicată 1966). Kent, însă, nu este de părere că restrângerea accesului altor persoane la informații reprezintă parte integrantă a activității de informații.
2. Kent, *Strategic Intelligence*, 3-4.
3. În timpul războiului este necesară folosirea unor mijloace tehnice şi secrete (cum sunt informările agenților sau comunicațiile interceptate) pentru obținerea unor informații privind condițiile meteorologice de pe teritoriul inamicului. Pentru aceste informații am putea folosi denumirea de "informații meteorologice secrete". Cu toate acestea, termenul "secrete" se referă la mijloacele prin care sunt obținute datele neprelucrate, nu la informațiile meteorologice care permit sau care stau la baza prognozei timpului probabil.
4. Aşa cum scria Willmoore Kendall în 1949 într-o recenzie a cărții lui Kent: "Cursul evenimentelor este perceput [de 'starea de spirit' reflectată în cartea lui Kent] nu ca un lucru care poate fi influențat, ci ca o bandă înregistrată aflată într-un aparat; iar sarcina serviciilor de informații este să afle ce este pe ea." "The Function of Intelligence", *World Politics 1*, nr. 6 (iulie 1949): 549.
5. Kent, *Strategic Intelligence*, viii [subliniere adăugată].
6. William E. Colby, "Intelligence for the 1980s", *The Information Society 1*, nr. 1 (1981): 59.
7. Pentru această interpretare a relației dintre informațiile secrete şi cele obținute din surse deschise, îi rămân îndatorat lui Michael Herman, de la Nuffield College, Oxford, care a introdus această propunere pe agenda Convenției din 1989 a Asociației pentru Studii Internaționale.

   De asemenea, informațiile obținute din surse deschise pot fi culese de o agenție secretă înainte ca acele informații să capete caracter secret. De exemplu, în timpul războiului, datele (cum sunt informațiile referitoare la sistemele de transport sau la rezervele de materiale strategice dintr-o anumită țară) care, pe timp de pace, sunt disponibile publicului larg capătă caracter de secret de stat, fiind astfel protejate de Guvern. În acest caz, culegerea informațiilor din surse deschise presupune evitarea potențialelor bariere de securitate care ar putea bloca accesul la informații pe viitor.
8. Avi Shlaim, "Failure in National Intelligence Estiamtes: The Case of the Yom Kippur War", *World Politics 28*, nr. 3 (aprilie 1976): 355.
9. Analiştii din serviciile de informații fac uneori diferență între "secrete" şi "mistere". Secretele sunt informații existente, la care nu există acces direct. Un

exemplu ar fi grosimea armurii noului tip de tancuri inamice; evident că inamicul deține această informație, dar face tot posibilul pentru a-i împiedica pe ceilalți să ajungă la această informație. Pe de altă parte, misterele sunt informațiile de care nimeni nu este sigur. De exemplu, va folosi oare inamicul noile tancuri pentru a-şi ataca vecinii în următorii zece ani? Chiar dacă inamicul s-a hotărât să atace peste trei ani, nu are de unde să ştie dacă nu se va răzgândi între timp. Kent sugerează că informațiile strategice cu caracter secret ar putea dezlega misterele sau, cel puțin, ar fi mult mai eficiente decât orice altă metodă.

10. Kent, *Strategic Intelligence*, 206-207.

11. În opinia lui Kent, acestea mai sunt cunoscute şi ca informații furnizate "pe loc" sau, mai informal, "la minut" (Kent, *Strategic Intelligence*, 28-29). Un serviciu de informații ca CIA-ul reprezintă un model de referință, având atribuții similare Serviciului pentru Cercetare din cadrul Bibliotecii Congresului American.

12. William E. Colby, *Honorable Men: My Life in the CIA* (New York: Simon and Schuster, 1978), 245.

Despre autori

Abraham N. Shulsky era membru marcant al Centrului de Informații pentru Strategia Națională (NSIC) din Washington, D.C., atunci când a scris *Războiul tăcut*. În prezent, lucrează la Washington unde este consultant pe probleme de securitate națională. Anterior, a făcut parte din echipa de planificare a strategiilor politice din cadrul cabinetului Ministrului Apărării. Mai mult decât atât, a ocupat funcția de director al politicii privind controlul strategic al armelor din cadrul Pentagonului şi funcția de director al echipei minoritare (democratice) din cadrul Comisiei Speciale pentru Informații a Senatului. De asemenea, a fost consultantul Consiliului de Experți pe probleme de Informații Externe al preşedintelui şi reprezentantul Ministrului Apărării la Negocierile pe Probleme Nucleare şi privind Spațiul Cosmic de la Geneva dintre SUA şi USSR. Dr. Shulsky este autorul mai multor articole referitoare la serviciile de informații şi probleme legate de securitatea națională.

Gary J. Schmitt este preşedintele Proiectului pentru Noul Secol American, un grup de experți cu sediul la Washington specializat pe probleme de securitate națională. A ocupat funcția de director executiv al Consiliului de Experți pe probleme de Informații Externe al preşedintelui şi funcția de director al echipei minoritare din cadrul Comisiei Speciale de Informații a Senatului. De asemenea, a fost consultant în cadrul Ministerului Apărării. Dr. Schmitt a scris multe lucrări referitoare la probleme de securitate națională şi guvernul american.